

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau

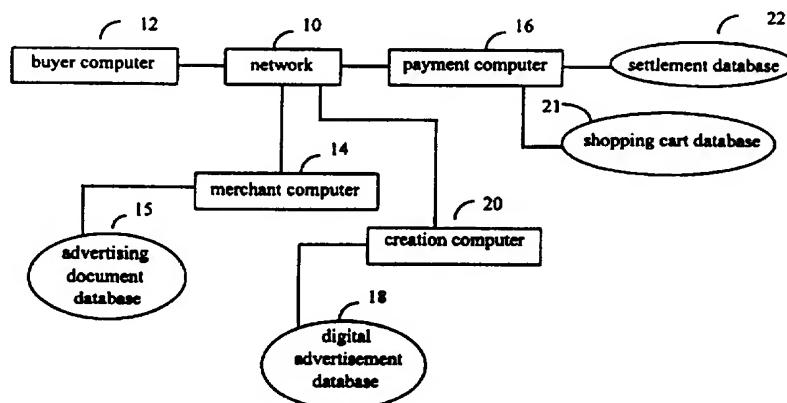


INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

|   |    |   |
|---|----|---|
| (51) International Patent Classification <sup>6</sup> :<br><b>G06F 17/60</b>  | A1 | (11) International Publication Number: <b>WO 96/13013</b><br>(43) International Publication Date: 2 May 1996 (02.05.96) |
| (21) International Application Number: PCT/US95/13723   |    | (81) Designated States: JP, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).           |
| (22) International Filing Date: 24 October 1995 (24.10.95)  |    |   |
| (30) Priority Data:<br>08/328,133 24 October 1994 (24.10.94) US   |    | Published<br><i>With international search report.</i>   |
| (71) Applicant: OPEN MARKET, INC. [US/US]; 245 First Street, Cambridge, MA 02142 (US).  |    |   |
| (72) Inventors: PAYNE, Andrew, C.; 5 Lewis Street, Lincoln, MA 01773 (US). STEWART, Lawrence, C.; One Arborwood Drive, Burlington, MA 01803 (US). MACKIE, David, J.; 8 Shepard Street #2, Cambridge, MA 02138 (US). |    |   |
| (74) Agent: WALPERT, Gary, A.; Fish & Richardson P.C., 225 Franklin Street, Boston, MA 02110 (US).  |    |   |

(54) Title: NETWORK SALES SYSTEM

buyer computer 12      merchant computer 14      payment computer 16



(57) Abstract

A network-based sales system includes at least one buyer computer (12) for operation by a user desiring to buy a product, at least one merchant computer (14), and at least one payment computer (16). The buyer computer is programmed to receive a user request for purchasing a product. The payment computer is programmed to receive the payment message, from the buyer computer, to cause an access message to be created that comprises the product identifier and an access message authenticator based on a cryptographic key, and to cause the access message to be sent to the merchant computer. The merchant computer is programmed to receive the access message, to verify the access message authenticator to ensure that the access message authenticator was created using the cryptographic key, and to send the product to the user desiring the product.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

|    |                          |    |  |    |                          |
|----|--------------------------|----|--|----|--------------------------|
| AT | Austria                  | GB | United Kingdom                           | MR | Mauritania               |
| AU | Australia                | GE | Georgia                                  | MW | Malawi                   |
| BB | Barbados                 | GN | Guinea                                   | NE | Niger                    |
| BE | Belgium                  | GR | Greece                                   | NL | Netherlands              |
| BF | Burkina Faso             | HU | Hungary                                  | NO | Norway                   |
| BG | Bulgaria                 | IE | Ireland                                  | NZ | New Zealand              |
| BJ | Benin                    | IT | Italy                                    | PL | Poland                   |
| BR | Brazil                   | JP | Japan                                    | PT | Portugal                 |
| BY | Belarus                  | KE | Kenya                                    | RO | Romania                  |
| CA | Canada                   | KG | Kyrgyzstan                               | RU | Russian Federation       |
| CF | Central African Republic | KP | Democratic People's Republic<br>of Korea | SD | Sudan                    |
| CG | Congo                    | KR | Republic of Korea                        | SE | Sweden                   |
| CH | Switzerland              | KZ | Kazakhstan                               | SI | Slovenia                 |
| CI | Côte d'Ivoire            | LI | Liechtenstein                            | SK | Slovakia                 |
| CM | Cameroon                 | LK | Sri Lanka                                | SN | Senegal                  |
| CN | China                    | LU | Luxembourg                               | TD | Chad                     |
| CS | Czechoslovakia           | LV | Latvia                                   | TG | Togo                     |
| CZ | Czech Republic           | MC | Monaco                                   | TJ | Tajikistan               |
| DE | Germany                  | MD | Republic of Moldova                      | TT | Trinidad and Tobago      |
| DK | Denmark                  | MG | Madagascar                               | UA | Ukraine                  |
| ES | Spain                    | ML | Mali                                     | US | United States of America |
| FI | Finland                  | MN | Mongolia                                 | UZ | Uzbekistan               |
| FR | France                   |    |  | VN | Viet Nam                 |
| GA | Gabon                    |    |  |    |                          |

- 1 -

NETWORK SALES SYSTEM

Background of the Invention

This invention relates to user-interactive network sales systems for implementing an open marketplace for goods or services over computer networks such as the Internet.

U.S. Patent Application Serial No. 08/168,519, filed December 16, 1993 by David K. Gifford and entitled "Digital Active Advertising," the entire disclosure of which is hereby incorporated herein in its entirety by reference, describes a network sales system that includes a plurality of buyer computers, a plurality of merchant computers, and a payment computer. A user at a buyer computer asks to have advertisements displayed, and the buyer computer requests advertisements from a merchant computer, which sends the advertisements to the buyer computer. The user then requests purchase of an advertised product, and the buyer computer sends a purchase message to the merchant computer. The merchant computer constructs a payment order that it sends to the payment computer, which authorizes the purchase and sends an authorization message to the merchant computer. When the merchant computer receives the authorization message it sends the product to the buyer computer.

The above-mentioned patent application also describes an alternative implementation of the network sales system in which, when the user requests purchase of an advertised product, the buyer computer sends a payment order directly to the payment computer, which sends an authorization message back to the buyer computer that includes an unforgeable certificate that the payment

- 2 -

order is valid. The buyer computer then constructs a purchase message that includes the unforgeable certificate and sends it to the merchant computer. When the merchant computer receives the purchase request it 5 sends the product to the buyer computer, based upon the pre-authorized payment order.

Summary of the Invention

In one aspect, the invention provides a network-based sales system that includes at least one buyer 10 computer for operation by a user desiring to buy a product, at least one merchant computer, and at least one payment computer. The buyer computer, the merchant computer, and the payment computer are interconnected by a computer network. The buyer computer is programmed to 15 receive a user request for purchasing a product, and to cause a payment message to be sent to the payment computer that comprises a product identifier identifying the product. The payment computer is programmed to receive the payment message, to cause an access message 20 to be created that comprises the product identifier and an access message authenticator based on a cryptographic key, and to cause the access message to be sent to the merchant computer. The merchant computer is programmed to receive the access message, to verify the access 25 message authenticator to ensure that the access message authenticator was created using the cryptographic key, and to cause the product to be sent to the user desiring to buy the product.

The invention provides a simple design 30 architecture for the network sales system that allows the merchant computer to respond to payment orders from the buyer computer without the merchant computer having to communicate directly with the payment computer to ensure that the user is authorized to purchase the product and 35 without the merchant computer having to store information

- 3 -

in a database regarding which buyers are authorized to purchase which products. Rather, when the merchant computer receives an access message from the buyer computer identifying a product to be purchased, the 5 merchant computer need only check the access message to ensure that it was created by the payment computer (thereby establishing for the merchant computer that the buyer is authorized to purchase the product), and then the merchant computer can cause the product to be sent to 10 the buyer computer who has been authorized to purchase the product.

In another aspect, the invention features a network-based sales system that includes at least one buyer computer for operation by a user desiring to buy 15 products, at least one shopping cart computer, and a shopping cart database connected to the shopping cart computer. The buyer computer and the shopping cart computer are interconnected by a computer network. The buyer computer is programmed to receive a plurality of 20 requests from a user to add a plurality of respective products to a shopping cart in the shopping cart database, and, in response to the requests to add the products, to send a plurality of respective shopping cart messages to the shopping cart computer each of which 25 includes a product identifier identifying one of the plurality of products. The shopping cart computer is programmed to receive the plurality of shopping cart messages, to modify the shopping cart in the shopping cart database to reflect the plurality of requests to add 30 the plurality of products to the shopping cart, and to cause a payment message associated with the shopping cart to be created. The buyer computer is programmed to receive a request from the user to purchase the plurality of products added to the shopping cart and to cause the 35 payment message to be activated to initiate a payment

- 4 -

transaction for the plurality of products added to the shopping cart.

In another aspect, the invention features a network-based link message system that includes at least 5 one client computer for operation by a client user and at least one server computer for operation by a server user. The client computer and the server computer are interconnected by a computer network. The client computer is programmed to send an initial link message to 10 the server computer. The server computer is programmed to receive the initial link message from the client computer and to create, based on information contained in the initial link message, a session link message that encodes a state of interaction between the client 15 computer and the server computer. The session link message includes a session link authenticator, computed by a cryptographic function of the session link contents, for authenticating the session link message. The server computer is programmed to cause the session link message 20 to be sent to the client computer. The client computer is programmed to cause the session link message to be sent to a computer in the network that is programmed to authenticate the session link message by examining the session link authenticator and that is programmed to 25 respond to the session link message based on the state of the interaction between the client computer and the server computer.

In another aspect, the invention features a network-based sales system that includes a merchant 30 database having a plurality of digital advertisements and a plurality of respective product fulfillment items, at least one creation computer for creating the merchant database, and at least one merchant computer for causing the digital advertisements to be transmitted to a user 35 and for causing advertised products to be transmitted to

- 5 -

the user. The creation computer and the merchant computer are interconnected by a computer network. The creation computer is programmed to create the merchant database, and to transmit the digital advertisements and 5 the product fulfillment items to the merchant computer. The merchant computer is programmed to receive the digital advertisements and product fulfillment items, to receive a request for a digital advertisement from a user, to cause the digital advertisement to be sent to 10 the user, to receive from the user an access message identifying an advertised product, and to cause the product to be sent to the user in accordance with a product fulfillment item corresponding to the product.

In another aspect, the invention features a 15 hypertext statement system that includes a client computer for operation by a client user and one or more server computers for operation by a server user. The client computer and the server computers are interconnected by a computer network. At least one of 20 the server computers is programmed to record purchase transaction records in a database. Each of the purchase transaction records includes a product description. The server computer is programmed to transmit a statement document that includes the purchase transaction records 25 to the client computer. The client computer is programmed to display the product descriptions, to receive a request from the client user to display a product corresponding to a product description displayed by the client computer, and to cause a product hypertext 30 link derived from a purchase transaction record to be activated. At least one of the server computers is programmed to respond to activation of the product hypertext link by causing the product to be sent to the client computer.

- 6 -

In another aspect, the invention features a network payment system that includes at least one buyer computer for operation by a user desiring to buy a product and at least one payment computer for processing payment messages from the buyer computer. The buyer computer and the payment computer are interconnected by a computer network. The buyer computer is programmed to cause a payment message to be sent to the payment computer. The payment message includes a product identifier identifying the product that the user desires to buy. The payment computer is programmed to receive the payment message, to cause an access message to be created to enable the user to access the product, and to record a purchase transaction record in the settlement database. The buyer computer is programmed to cause a request for purchase transaction records to be sent to the payment computer. The payment computer is programmed to receive the request for purchase transaction records and to cause a document derived from the purchase transaction records to be sent to the buyer computer.

Brief Description of the Drawings

Fig. 1 is a block diagram of a network sales system in accordance with the present invention.

Fig. 2 (2-A through 2-I) is a flowchart diagram illustrating the operation of a purchase transaction in the network sales system of Fig. 1.

Fig. 3 (3-A through 3-B) is a flowchart diagram illustrating the use of a shopping cart for the purchase of products in connection with the network sales system of Fig. 1.

Fig. 4 (4-A through 4-C) is a flowchart diagram illustrating the operation of a smart statement in the network sales system of Fig. 1.

- 7 -

Fig. 5 is a screen snapshot of an advertising document that the merchant computer sends to the buyer computer in Fig. 2.

Fig. 6 is a screen snapshot of a confirmation 5 document that the payment computer sends to the buyer computer in Fig. 2.

Fig. 7 is a screen snapshot of a new account document that the payment computer sends to the buyer computer in Fig. 2.

10 Fig. 8 is a screen snapshot of an account name prompt that the buyer computer creates in Fig. 2.

Fig. 9 is a screen snapshot of a document that the payment computer sends to the buyer computer in Fig. 2 and that provides an option either to repurchase or to 15 use a previously purchased access.

Fig. 10 is a screen snapshot of a fulfillment document that the merchant computer sends to the buyer computer in Fig. 2.

Fig. 11 is a screen snapshot of a smart statement 20 document that the payment computer sends to the buyer computer in Fig. 4.

Figs. 12 and 13 are screen snapshots of a transaction detail document that the payment computer sends to the buyer computer in Fig. 4.

25 Fig. 14 is a screen snapshot of a customer service form that the payment computer sends to the buyer computer in Fig. 4.

#### Detailed Description

With reference to Fig. 1, a network sales system 30 in accordance with the present invention includes a buyer computer 12 operated by a user desiring to buy a product, a merchant computer 14, which may be operated by a merchant willing to sell products to the buyer or by a manager of the network sales system, a payment computer 35 16 typically operated by a manager of the network sales

- 8 -

system, and a creation computer 20 typically operated by the merchant. The buyer, merchant, payment, and creation computers are all inter-connected by a computer network 10 such as the Internet.

5 Creation computer 20 is programmed to build a "store" of products for the merchant. A printout of a computer program for use in creating such a "store" in accordance with the present invention is provided as Appendix F.

10 The products advertised by merchant computer 14 may be, for example, newspaper or newsletter articles available for purchase by buyers. Creation computer 20 creates a digital advertisement database 18 that stores advertising documents (which may for example be in the 15 form of summaries of newspaper or newsletter articles, accompanied by prices) and product fulfillment items (which may be the products themselves if the products can be transmitted over the network, or which may be hard goods identifiers if the products are hard goods, i.e., 20 durable products as opposed to information products). Creation computer 20 transmits contents of the advertising document database 18 to merchant computer 14 to enable the merchant computer to cause advertisements and products to be sent to buyers. Merchant computer 14 25 maintains advertising documents locally in advertising document database 15. In an alternative embodiment, the creation computer does not have a local digital advertisement database, but instead updates a remote advertising document database on a merchant computer. 30 These updates can be accomplished using HTML forms or other remote database technologies as is understood by practitioners of the art.

Payment computer 16 has access to a settlement database 22 in which payment computer 16 can record 35 details of purchase transactions. The products may be

- 9 -

organized into various "domains" of products, and payment computer 16 can access settlement database 22 to record and retrieve records of purchases of products falling within the various domains. Payment computer 16 also has 5 access to a shopping cart database 21 in which a "shopping cart" of products that a user wishes to purchase can be maintained as the user shops prior to actual purchase of the contents of the shopping cart.

With reference to Fig. 2, a purchase transaction 10 begins when a user at buyer computer 12 requests advertisements (step 24) and buyer computer 12 accordingly sends an advertising document URL (universal resource locator) to merchant computer 14 (step 26). The merchant computer fetches an advertising document from 15 the advertising document database (step 28) and sends it to the buyer computer (step 30). An example of an advertising document is shown in Fig. 5. Details of URLs and how they are used are found in the microfiche Appendix G.

20 The user browses through the advertising document and eventually requests a product (step 32). This results in the buyer computer sending payment URL A to the payment computer (step 34). Payment URL A includes a product identifier that represents the product the user 25 wishes to buy, a domain identifier that represents a domain of products to which the desired product belongs, a payment amount that represents the price of the product, a merchant computer identifier that represents merchant computer 14, a merchant account identifier that 30 represents the particular merchant account to be credited with the payment amount, a duration time that represents the length of time for which access to the product is to be granted to the user after completion of the purchase transaction, an expiration time that represents a 35 deadline beyond which this particular payment URL cannot

- 10 -

be used, a buyer network address, and a payment URL authenticator that is a digital signature based on a cryptographic key. The payment URL authenticator is a hash of other information in the payment URL, the hash 5 being defined by a key shared by the merchant and the operator of the payment computer.

In an alternative embodiment, step 34 consists of the buyer computer sending a purchase product message to the merchant computer, and the merchant computer provides 10 payment URL A to the buyer computer in response to the purchase product message. In this alternative embodiment, payment URL A contains the same contents as above. The buyer computer then sends the payment URL A it has received from the merchant computer to the payment 15 computer.

When the payment computer receives the payment URL it verifies whether the payment URL authenticator was created from the contents of the payment URL using the cryptographic key (step 36). If not, the payment 20 computer sends a document to the buyer computer indicating that access to the network sales system is denied (step 38). Otherwise, the payment computer determines whether the expiration time has past (step 40). If it has, the payment computer sends a document to 25 the buyer computer indicating that the time has expired (step 41). Otherwise, the payment computer checks the buyer computer network address to see if it matches the one specified in the payment URL (step 42). If it does not match, the payment computer sends a document to the 30 buyer computer indicating that access to the network payment system is denied (step 43). Otherwise, the payment computer sends a payment confirmation document to the buyer computer, the payment confirmation document including an "open" link and a "continue" link (step 44).

- 11 -

An example of a confirmation document is shown in Fig. 6. The confirmation document asks the user to click on a "continue" button if the user already has an account with the payment computer, or to click on an "open" 5 button if the user does not already have an account and wishes to open one.

If the user clicks on the "open" button (step 46), the buyer computer sends payment URL C to the payment computer (step 48), payment URL C being similar to 10 payment URL A but also indicating that the user does not yet have an account. The payment computer creates a new account document (step 50) and sends it to the buyer computer (step 52). An example of a new account document is shown in Fig. 7. When the user receives the new 15 account document he enters the new account name, an account password, a credit card number, the credit card expiration date, and security information such as the maiden name of the user's mother (step 54), and presses a "submit" button (not shown in Fig. 7). The buyer 20 computer sends the new account information to the payment computer (step 56), which enters the new account in the settlement database (step 58).

If the user clicks on the "continue" button (step 60), the buyer computer sends payment URL B to the 25 payment computer (step 62), payment URL B being similar to payment URL A but also indicating that the user already has an account. The payment computer then instructs the buyer computer to provide the account name and password (steps 64 and 66), and the buyer computer 30 prompts the user for this information by creating an account name prompt (example shown in Fig. 8) and a similar password prompt. The user enters the information (step 68) and the buyer computer sends the account name and password to the payment computer (step 70).

- 12 -

The payment computer verifies whether the user name and password are correct (step 72). If they are not correct, the payment computer sends a document to the buyer computer indicating that access to the network sales system is denied (step 74). Otherwise, the payment computer determines whether additional security is warranted, based on, e.g., whether the payment amount exceeds a threshold (step 73). If additional security is warranted, the payment computer creates a challenge form document and sends it to the buyer computer (step 75). The user enters the security information (step 77), the buyer computer sends the security information to the payment computer (step 79), and the payment computer determines whether the security information is correct (step 81). If it is not correct, the payment computer sends a document to the buyer computer indicating that access to the network sales system is denied (step 83).

If the security information is correct, or if additional security was not warranted, the payment computer checks the settlement database to determine whether the user has unexpired access to the domain identifier contained in the payment URL (step 82). If so, the payment computer sends to the buyer computer a document providing an option either to repurchase or to use the previously purchased access (step 84). An example of such a document is shown in Fig. 9. The user can respond to the recent purchase query document by choosing to access the previously purchased document (step 85) or to go ahead and buy the currently selected product (step 86).

If the user chooses to access the previously purchased document, the buyer computer skips to step 92 (see below). If the user chooses to buy the currently selected product, the payment computer calculates an actual payment amount that may differ from the payment

- 13 -

amount contained in the payment URL (step 87). For example, the purchase of a product in a certain domain may entitle the user to access other products in the domain for free or for a reduced price for a given period 5 of time.

The payment computer then verifies whether the user account has sufficient funds or credit (step 76). If not, the payment computer sends a document to the buyer computer indicating that the user account has 10 insufficient funds (step 78). Otherwise, the payment computer creates an access URL (step 80) that includes a merchant computer identifier, a domain identifier, a product identifier, an indication of the end of the duration time for which access to the product is to be 15 granted, the buyer network address, and an access URL authenticator that is a digital signature based on a cryptographic key. The access URL authenticator is a hash of other information in the access URL, the hash being defined by a key shared by the merchant and the 20 operator of the payment computer. The payment computer then records the product identifier, the domain, the user account, the merchant account, the end of duration time, and the actual payment amount in the settlement database (step 88).

25 The payment computer then sends a redirect to access URL to the buyer computer (step 90), which sends the access URL to the merchant computer (step 92). The merchant computer verifies whether the access URL authenticator was created from the contents of the access 30 URL using the cryptographic key (step 94). If not, the merchant computer sends a document to the buyer computer indicating that access to the product is denied (step 96).

Otherwise, the merchant computer verifies whether 35 the duration time for access to the product has expired

- 14 -

(step 98). This is done because the buyer computer can request access to a purchased product repeatedly. If the duration time has expired, the merchant computer sends a document to the buyer computer indicating that the time 5 has expired (step 100). Otherwise the merchant computer verifies that the buyer computer network address is the same as the buyer network address in the access URL (step 101), and if so, sends a fulfillment document to the buyer computer (step 102), which is displayed by the 10 buyer computer (step 104). An example of a fulfillment document is shown in Fig. 10. Otherwise, the merchant computer sends a document to the buyer computer indicating that access is not allowed (step 103).

With reference now to Fig. 3, when the merchant 15 computer sends the advertising document to the buyer computer, the user may request that a product be added to a shopping cart in the shopping cart database rather than request that the product be purchased immediately. The buyer computer sends a shopping cart URL to the payment 20 computer (step 108), the shopping cart URL including a product identifier, a domain identifier, a payment amount, a merchant computer identifier, a merchant account identifier, a duration time, an expiration time, and a shopping cart URL authenticator that is a digital 25 signature based on a cryptographic key. The shopping cart URL authenticator is a hash of other information in the shopping cart URL, the hash being defined by a key shared by the merchant and the operator of the payment computer.

30 The payment computer verifies whether the shopping cart URL authenticator was created from the contents of the shopping cart URL using a cryptographic key (step 110). If not, the payment computer sends a document to the buyer computer indicating that access to the network 35 sales system is denied (step 112). Otherwise, before any

- 15 -

modification to a user's shopping cart is allowed, user authentication is performed (step 113) in a manner analogous to steps 40-81. Once the user is authenticated, the payment computer creates or updates a 5 payment URL for the shopping cart (step 114).

The user then either requests more advertisements (step 24 in Fig. 2) and possibly adds another product to the shopping cart, requests display of the shopping cart (step 116), or requests purchase of the entire contents 10 of the shopping cart (step 124). If the user requests display of the shopping cart (step 116), the buyer computer sends a fetch shopping cart request to the payment computer (step 118), and the payment computer and buyer computer (step 119) perform steps analogous to 15 steps 64-81. The payment computer returns the contents of the shopping cart to the buyer computer (step 120), which displays the contents of the shopping cart (step 122). If the user requests that the entire contents of the shopping cart be purchased (step 124) the buyer 20 computer causes the payment URL for the shopping cart to be activated (step 126) and the payment URL is processed in a manner analogous to the processing of payment URLs for individual products (beginning with step 36 in Fig. 2).

25 With reference now to Fig. 4, a user can request display of a "smart statement" that lists purchase transactions for a given month (step 128). When the buyer computer receives such a request, it sends a smart statement URL to the payment computer (step 130).

30 When the payment computer receives the smart statement URL, it verifies whether the smart statement URL authenticator was created from the contents of the smart statement URL using a cryptographic key (step 132). If not, the payment computer sends a document to the 35 buyer computer indicating that access is denied (step

- 16 -

134). Otherwise, the payment computer checks to determine whether the buyer network address in the smart statement URL matches the buyer computer's actual network address (step 136). If not, the payment computer sends a 5 document to the buyer computer indicating that access is denied (step 138). Otherwise (step 140), the payment computer and buyer computer perform a set of steps analogous to steps 64-81 in Fig. 2 (payment computer requests account name and password, user provides the 10 requested information, and payment computer verifies the information).

In an alternative embodiment steps 132-138 are omitted.

After verification of account information is 15 complete, the payment computer retrieves the requested settlement data from the settlement database, creates a smart statement document for the buyer, and sends the smart statement document to the buyer computer (step 142). An example of a smart statement document is shown 20 in Fig. 11. Each purchase transaction record in the smart statement document includes the data of the transaction, the name of the merchant, an identification of the product, and the payment amount for the product. The smart statement document also includes a transaction 25 detail URL for each purchase transaction (these URLs, or hypertext links, are discussed below and are not shown in Fig. 11). The smart statement document also identifies previous statements that the user may wish to have displayed.

30 The buyer computer displays the retrieved document (step 144), and the user may request transaction details for a particular transaction listed on the smart statement (step 146). If so, the buyer computer sends a transaction detail URL (or "payment detail URL") to the 35 payment computer (step 148). The transaction detail URL

- 17 -

includes a transaction identifier, a buyer network address, and a transaction detail URL authenticator. When the payment computer receives the transaction detail URL, it performs (step 150) a set of steps analogous to 5 steps 132-140 (verification of URL authenticator, buyer network address, and account information). The payment computer then retrieves from the settlement database data corresponding to the payment transaction specified in the transaction detail URL, creates a transaction detail 10 document, and sends it to the buyer computer (step 152).

An example of a transaction detail document is shown in Figs. 12 and 13. The document displays a number of items of information about the transaction, including the transaction date, end of the duration time 15 ("expiration"), a description of the product, the payment amount, the domain corresponding to the product, an identification of the merchant, and the merchant's address.

The smart statement document and the transaction detail document both include customer service URLs (hypertext links) that allow the user to request customer service (i.e., to send comments and suggestions to the payment computer). When the user requests customer service (step 154), the buyer computer sends the customer 20 service URL to the payment computer (step 156), which creates a customer service form and sends it to the buyer computer (step 158). An example of a customer service form is shown in Fig. 14. The user types comments into the customer service form (step 160), and the buyer 25 computer sends the user's comments to the payment computer (step 162). The payment computer then posts the user comments and sends a thank you document to the buyer computer (step 164).

A user may request display of a product included 30 in the smart statement. When the user requests that the

- 18 -

product be displayed (step 166), the buyer computer sends the access URL contained in the smart statement document to the merchant computer (step 168), and the buyer computer and merchant computer perform a set of steps 5 analogous to steps 94-104 in Fig. 2 (authentication of access URL, verification whether duration time has expired, verification of buyer network address, and transmission of fulfillment document to buyer computer).

Whenever the present application states that one 10 computer sends a URL to another computer, it should be understood that in preferred embodiments the URL is sent in a standard HTTP request message, unless a URL message is specified as a redirection in the present application. The request message includes components of the URL as 15 described by the standard HTTP protocol definition. These URL components in the request message allow the server to provide a response appropriate to the URL. The term "URL" as used the present application is an example of a "link," which is a pointer to another document or 20 form (including multimedia documents, hypertext documents including other links, or audio/video documents).

When the present application states that one computer sends a document to another computer, it should be understood that in preferred embodiments the document 25 is a success HTTP response message with the document in the body of the message. When the present application states that a server sends an account name and password request message to the client, it should be understood that in preferred embodiments the account name and 30 password request message is an unauthorized HTTP response. A client computer sends account name and password information to a server as part of a request message with an authorization field.

The software architecture underlying the 35 particular preferred embodiment is based upon the

- 19 -

hypertext conventions of the World Wide Web. For example, the Hypertext Markup Language (HTML) document format is used to represent digital advertisements. The HTML forms fill out support is used in Mosaic 2.0. The 5 Hypertext Transfer Protocol (HTTP) is used between buyer and merchant computers. Documents are named with Uniform Resource Locators (URLs) in the network of computers. URLs are authenticated using digital signatures.

There has been described a new and useful network 10 based sales system. It is apparent that those skilled in the art may make numerous modifications and departures from the specific embodiments described herein without departing from the spirit and scope of the claimed invention.

- 20 -

CLAIMS

1. A network-based sales system, comprising:
  - at least one buyer computer for operation by a user desiring to buy a product;
  - 5 at least one merchant computer; and
  - at least one payment computer;
  - said buyer computer, said merchant computer, and said payment computer being interconnected by a computer network;
- 10 said buyer computer being programmed to receive a user request for purchasing a product, and to cause a payment message to be sent to said payment computer that comprises a product identifier identifying said product;
- 15 said payment computer being programmed to receive said payment message, to cause an access message to be created that comprises said product identifier and an access message authenticator based on a cryptographic key, and to cause said access message to be sent to said merchant computer; and
- 20 said merchant computer being programmed to receive said access message, to verify said access message authenticator to ensure that said access message authenticator was created using said cryptographic key, and to cause said product to be sent to said user
- 25 desiring to buy said product.

2. A network-based sales system in accordance with claim 1, wherein said payment message and said access message each comprises a universal resource locator.

- 30 3. A network-based sales system in accordance with claim 1, wherein said payment computer is programmed to identify said merchant computer upon receipt of said payment message from said buyer computer.

- 21 -

4. A network-based sales system in accordance with claim 1, wherein said access message comprises a buyer network address.

5 5. A network-based sales system in accordance with claim 4, wherein:

said product can be transmitted from one computer to another; and

10 said merchant computer causes said product to be sent to said user by transmitting said product to said buyer network address only.

6. A network-based sales system in accordance with claim 4, wherein said merchant computer is programmed to verify whether said buyer network address in said access message matches the actual network address 15 of said buyer computer.

7. A network-based sales system in accordance with claim 1, wherein said payment message comprises a buyer network address.

20 8. A network-based sales system in accordance with claim 7, wherein said payment computer is programmed to verify whether said buyer network address in said payment message matches the actual network address of said buyer computer.

25 9. A network-based sales system in accordance with claim 1, wherein said access message authenticator comprises a cryptographic function of contents of said access message based on said cryptographic key.

10. A network-based sales system in accordance with claim 1, wherein said payment computer is programmed

- 22 -

to verify said payment message authenticator to ensure that said payment message authenticator was created using said cryptographic key.

11. A network-based sales system in accordance  
5 with claim 10, wherein said payment message authenticator comprises a cryptographic function of contents of said payment message based on said cryptographic key.

12. A network-based sales system in accordance with claim 1, wherein said payment message comprises a  
10 payment amount.

13. A network-based sales system in accordance with claim 1, wherein said payment message comprises a merchant account identifier that identifies a merchant account.

15 14. A network-based sales system in accordance with claim 1, wherein said buyer computer is programmed to transmit a user account identifier to said payment computer that identifies a user account.

15. A network-based sales system in accordance  
20 with claim 14, wherein:

    said payment message comprises a payment amount;  
    and

    said payment computer is programmed to ensure that  
    said user account has sufficient funds or credit to cover  
25 said payment amount.

16. A network-based sales system in accordance with claim 14, wherein:

- 23 -

5 said payment message comprises a payment amount and a merchant account identifier that identifies a merchant account; and

5 payment amount, said user account, and said merchant account in a settlement database.

17. A network-based sales system in accordance with claim 16, wherein:

10 said payment message comprises a domain identifier; and

5 said payment computer is programmed to record said domain identifier and said user account in a settlement database.

18. A network-based sales system in accordance with claim 17, wherein said payment computer is programmed to check said settlement database, upon receipt of said payment message, to determine whether said user account has previously purchased a product associated with said domain identifier.

20 19. A network-based sales system in accordance with claim 18, wherein said payment computer is programmed to determine an actual payment amount for said product identified by said product identifier in said payment message based on whether said user account has 25 previously purchased a product associated with said domain identifier.

20. A network-based sales system in accordance with claim 1, wherein said buyer computer is programmed to transmit a user authenticator to said payment computer and said payment computer is programmed to verify said user authenticator.

- 24 -

21. A network-based sales system in accordance with claim 20, wherein said user authenticator comprises a password.

22. A network-based sales system in accordance 5 with claim 20, wherein:

    said buyer computer is programmed to transmit security information to said payment computer;

    said payment computer is programmed to transmit a challenge form to said buyer computer under a 10 predetermined condition, said challenge form asking for said security information previously transmitted by said buyer computer to said payment computer;

    said payment computer is programmed to respond to said challenge form by querying said user for said 15 security information and transmitting said security information to said payment computer; and

    said payment computer is programmed to verify authenticity of said security information.

23. A network-based sales system in accordance 20 with claim 22, wherein:

    said payment message comprises a payment amount; and

    said predetermined condition comprises receipt of a payment amount in said payment message that exceeds a 25 threshold.

24. A network-based sales system in accordance with claim 1, wherein said payment message comprises a merchant computer identifier that identifies said merchant computer.

- 25 -

25. A network-based sales system in accordance with claim 24, wherein said access message comprises said merchant computer identifier.

26. A network-based sales system in accordance 5 with claim 1, wherein said payment message comprises a duration time that specifies a length of time for which access to said product is to be granted.

27. A network-based sales system in accordance with claim 26, wherein said payment computer is 10 programmed to use said duration time to compute an end of duration time and to cause said end of duration time to be included in said access message.

28. A network-based sales system in accordance with claim 27, wherein said merchant computer is 15 programmed to verify, upon receipt of said access message, that said end of duration time has not past.

29. A network-based sales system in accordance with claim 1, wherein said payment message comprises an expiration time after which said payment message can no 20 longer be used.

30. A network-based sales system in accordance with claim 29, wherein said payment computer is programmed to verify, upon receipt of said payment message, that said expiration time has not past.

31. A network-based sales system in accordance 25 with claim 1, wherein:

    said payment computer is programmed to cause said access message to be sent to said buyer computer; and

- 26 -

      said buyer computer is programmed to cause said access message received from said payment computer to be sent to said merchant computer.

32. A network-based sales system, comprising:  
5       at least one buyer computer for operation by a user desiring to buy a product;  
       at least one merchant computer; and  
       at least one payment computer;  
       said buyer computer, said merchant computer, and  
10      said payment computer being interconnected by a computer network;  
       said buyer computer being programmed to receive a user request for purchasing a product, and to cause a payment URL to be sent to said payment computer that  
15      comprises a product identifier identifying said product, a payment amount, and a payment URL authenticator comprising a cryptographic function of contents of said payment URL based on a cryptographic key;  
       said payment computer being programmed to receive  
20      said payment URL, to verify said payment URL authenticator to ensure that said payment URL authenticator was created using said cryptographic key, to ensure that said user has sufficient funds or credit to cover said payment amount, to identify said merchant  
25      computer operated by said merchant willing to sell said product to said buyer, to cause an access URL to be created that comprises said product identifier and an access URL authenticator comprising a cryptographic function of contents of said access URL based on a  
30      cryptographic key, and to cause said access URL to be sent to said buyer computer;  
       said buyer computer being programmed to cause said access URL received from said payment computer to be sent to said merchant computer; and

- 27 -

said merchant computer being programmed to receive said access URL, to verify said access URL authenticator to ensure that said access URL authenticator was created using said cryptographic key, and to cause said product 5 to be sent to said user desiring to buy said product.

33. A method of operating a payment computer in a computer network comprising at least one buyer computer for operation by a user desiring to buy a product, at least one merchant computer, and at least one payment 10 computer, the method comprising the steps of:

receiving, at said payment computer, a payment message that said buyer computer has caused to be sent to said payment computer in response to a user request for purchasing a product, said payment message comprising a 15 product identifier identifying said product;

causing an access message to be created that comprises said product identifier and an access message authenticator based on a cryptographic key; and

causing said access message to be sent to said 20 merchant computer, said merchant computer being programmed to receive said access message, to verify said access message authenticator to ensure that said access message authenticator was created using said cryptographic key, and to cause said product to be sent 25 to said user desiring to buy said product.

34. A network-based sales system, comprising: at least one buyer computer for operation by a user desiring to buy products;

30 at least one shopping cart computer; and a shopping cart database connected to said shopping cart computer;

said buyer computer and said shopping cart computer being interconnected by a computer network;

- 28 -

5        said buyer computer being programmed to receive a plurality of requests from a user to add a plurality of respective products to a shopping cart in said shopping cart database, and, in response to said requests to add said products, to send a plurality of respective shopping cart messages to said shopping cart computer each of which comprises a product identifier identifying one of said plurality of products;

10      said shopping cart computer being programmed to receive said plurality of shopping cart messages, to modify said shopping cart in said shopping cart database to reflect said plurality of requests to add said plurality of products to said shopping cart, and to cause a payment message associated with said shopping cart to 15 be created; and

20      said buyer computer being programmed to receive a request from said user to purchase said plurality of products added to said shopping cart and to cause said payment message to be activated to initiate a payment transaction for said plurality of products added to said shopping cart.

25      35. A network-based sales system in accordance with claim 34, wherein said shopping cart computer is programmed to cause said payment message to be created before said buyer computer causes said payment message to be activated.

30      36. A network-based sales system in accordance with claim 34, wherein said buyer computer is programmed to receive a request from said user to display said plurality of products added to said shopping cart.

37. A network-based sales system in accordance with claim 36, wherein said buyer computer is programmed

- 29 -

to transmit a fetch shopping cart request to said payment computer in response to receipt of said request from said user.

38. A network-based sales system in accordance

5 with claim 37, wherein:

said payment computer is programmed to respond to said fetch shopping cart request by transmitting a message to said buyer computer indicating said plurality of products added to said shopping cart; and

10 said buyer computer is programmed to display said plurality of products added to said shopping cart.

39. A method of operating a shopping cart

computer in a computer network comprising at least one buyer computer for operation by a user desiring to buy 15 products, at least one shopping cart computer, and a shopping cart database connected to said shopping cart computer, said method comprising the steps of:

receiving, at said shopping cart computer, a plurality of shopping cart messages sent to said shopping 20 cart computer by said buyer computer in response to receipt of a plurality of requests from a user to add a plurality of respective products to a shopping cart in said shopping cart database, each of said shopping cart messages comprising a product identifier identifying one 25 of said plurality of products;

modifying said shopping cart in said shopping cart database to reflect said plurality of requests to add said plurality of products to said shopping cart; and causing a payment message associated with said

30 shopping cart to be created;

said buyer computer being programmed to receive a request from said user to purchase said plurality of products added to said shopping cart and to cause said

- 30 -

payment message to be activated to initiate a payment transaction for said plurality of products added to said shopping cart.

40. A network-based link message system,  
5 comprising:  
at least one client computer for operation by a  
client user; and  
at least one server computer for operation by a  
server user;  
10 said client computer and said server computer  
being interconnected by a computer network;  
said client computer being programmed to send an  
initial link message to said server computer;  
said server computer being programmed to receive  
15 said initial link message from said client computer, to  
create, based on information contained in said initial  
link message, a session link message that encodes a state  
of interaction between said client computer and said  
server computer, said session link message comprising a  
20 session link authenticator, computed by a cryptographic  
function of said session link contents, for  
authenticating said session link message, and to cause  
said session link message to be sent to said client  
computer;  
25 said client computer being programmed to cause  
said session link message to be sent to a computer in  
said network that is programmed to authenticate said  
session link message by examining said session link  
authenticator and that is programmed to respond to said  
30 session link message based on said state of said  
interaction between said client computer and said server  
computer.

- 31 -

41. A network-based link message system in accordance with claim 40, wherein:

    said client computer comprises a buyer computer for operation by a user desiring to buy a product;

5      said server computer comprises a payment computer for operation by a manager of said network-based link message system; and

10     said network-based link message system further comprises a merchant computer for operation by a merchant willing to sell said product to said buyer.

42. A network-based link message system in accordance with claim 41, wherein said computer that is programmed to authenticate said session link message comprises said merchant computer.

15     43. A network-based link message system in accordance with claim 41, wherein said initial link message comprises a payment message to said payment computer that comprises a product identifier identifying said product.

20     44. A network-based link message system in accordance with claim 43, wherein said session link message comprises an access message that comprises said product identifier to be created.

25     45. A network-based link message system in accordance with claim 44, wherein said merchant computer is programmed to respond to said access message by causing said product to be sent to said user desiring to buy said product.

30     46. A network-based link message system in accordance with claim 40, wherein said initial link

- 32 -

message and said session link message comprise universal resource locators.

47. A network-based link message system in accordance with claim 40, wherein:

5       said session link authenticator comprises a cryptographic function of contents of said session link message based on a cryptographic key; and  
          said computer to which said client computer is programmed to cause said session link message to be sent  
10      is programmed to verify that said session link authenticator was created using said cryptographic key.

48. A method of operating a server computer in a network-based link message system comprising at least one client computer for operation by a client user and at 15 least one server computer for operation by a server user, said client computer and said server computer being interconnected by a computer network, said method comprising the steps of:

receiving, at said server computer, an initial 20 link message sent to said server computer by said client computer;

creating, based on information contained in said initial link message, a session link message that encodes a state of interaction between said client computer and 25 said server computer, said session link message comprising a session link authenticator, computed by a cryptographic function of said session link contents, for authenticating said session link message; and

causing said session link message to be sent to 30 said client computer;

      said client computer being programmed to cause said session link message to be sent to a computer in said network that is programmed to authenticate said

- 33 -

session link message by examining said session link authenticator and that is programmed to respond to said session link message based on said state of said interaction between said client computer and said server

5 computer.

49. A network-based sales system, comprising:  
a merchant database comprising a plurality of digital advertisements and a plurality of respective product fulfillment items;

10 at least one creation computer for creating said merchant database; and

at least one merchant computer for causing said digital advertisements to be transmitted to a user and for causing advertised products to be transmitted to said

15 user;

said creation computer and said merchant computer being interconnected by a computer network;

20 said creation computer being programmed to create said merchant database, and to transmit said digital advertisements and said product fulfillment items to said merchant computer;

25 said merchant computer being programmed to receive said digital advertisements and product fulfillment items, to receive a request for a digital advertisement from a user, to cause said digital advertisement to be sent to said user, to receive from said user an access message identifying an advertised product, and to cause said product to be sent to said user in accordance with a product fulfillment item corresponding to said product.

30 50. A network-based sales system in accordance with claim 49, wherein each of said digital advertisements comprises an abstract of a product and a price.

- 34 -

51. A network-based sales system in accordance with claim 50, wherein:

at least one of said product fulfillment items comprises a product itself; and

5 said creation computer is programmed to transmit said product to said merchant computer with said digital advertisements.

52. A network-based sales system in accordance with claim 50, wherein:

10 at least one of said product fulfillment items comprises a hard good identifier; and

said creation computer is programmed to transmit said hard good identifier to said merchant computer with said digital advertisements.

15 53. A method of operating a merchant computer in a network-based sales system comprising a merchant database that comprises a plurality of digital advertisements and a plurality of respective product fulfillment items, at least one creation computer for  
20 creating said merchant database, and at least one merchant computer for causing said digital advertisements to be transmitted to a user and for causing advertised products to be transmitted to said user, said creation computer and said merchant computer being interconnected  
25 by a computer network, said method comprising the steps of:

30 receiving, at said merchant computer, said digital advertisements and said product fulfillment items, said digital advertisements and said product fulfillment items having been transmitted to said merchant computer by said creation computer, said merchant database comprising said digital advertisements and said product fulfillment items having been created by said creation computer;

- 35 -

receiving a request for a digital advertisement from a user;

causing said digital advertisement to be sent to said user;

5 receiving from said user an access message identifying an advertised product; and

causing said product to be sent to said user in accordance with a product fulfillment item corresponding to said product.

10 54. A hypertext statement system, comprising: a client computer for operation by a client user; and

one or more server computers for operation by a server user;

15 said client computer and said server computers being interconnected by a computer network;

at least one of said server computers being programmed to record purchase transaction records in a database, each of said purchase transaction records comprising a product description, and to transmit a statement document comprising said purchase transaction records to said client computer;

20 said client computer being programmed to display said product descriptions, to receive a request from said 25 client user to display a product corresponding to a product description displayed by said client computer, and to cause a product hypertext link derived from a purchase transaction record to be activated;

25 at least one of said server computers being programmed to respond to activation of said product 30 hypertext link by causing said product to be sent to said client computer.

- 36 -

55. A hypertext statement system in accordance with claim 54, wherein:

    said client computer is programmed to receive a request from said client user to display transaction

5 details corresponding to a product description displayed by said client computer and to cause a transaction detail hypertext link corresponding to said product description to be activated; and

    said server computer is programmed to respond to 10 activation of said transaction detail hypertext link by transmitting said transaction details to said client computer as a transaction detail document.

56. A hypertext statement system in accordance with claim 55, wherein:

15      said transaction detail document further comprises a customer service form hypertext link;

    said client computer is programmed to receive a request from said client user to display a customer service form and to cause said customer service form 20 hypertext link to be activated; and

    said server computer is programmed to respond to activation of said customer service form hypertext link by transmitting said customer service form to said client computer.

25      57. A hypertext statement system in accordance with claim 54, wherein:

    said statement document further comprises a customer service form hypertext link;

    said client computer is programmed to receive a 30 request from said client user to display a customer service form and to cause said customer service form hypertext link to be activated; and

- 37 -

      said server computer is programmed to respond to activation of said customer service form hypertext link by transmitting said customer service form to said client computer.

5       58. A method of operating a server computer in a hypertext statement system comprising a client computer for operation by a client user, and one or more server computers for operation by a server user, said client computer and said server computers being interconnected 10 by a computer network, said method comprising the steps of:

      recording, at one of said server computers, purchase transaction records in a database, each of said purchase transaction records comprising a product

15 description; and

      transmitting a statement document comprising said purchase transaction records to said client computer;

      said client computer being programmed to display said product descriptions, to receive a request from said 20 client user to display a product corresponding to a product description displayed by said client computer, and to cause a product hypertext link derived from a purchase transaction record to be activated;

      at least one of said server computers being 25 programmed to respond to activation of said product hypertext link by causing said product to be sent to said client computer.

59. A network payment system, comprising:

      at least one buyer computer for operation by a 30 user desiring to buy a product; and

      at least one payment computer for processing payment messages from said buyer computer;

- 38 -

    said buyer computer and said payment computer being interconnected by a computer network;

    said buyer computer being programmed to cause a payment message to be sent to said payment computer, said

5 payment message comprising a product identifier identifying said product that said user desires to buy;

    said payment computer being programmed to receive said payment message, to cause an access message to be created to enable said user to access said product, and

10 to record a purchase transaction record in said settlement database;

    said buyer computer being programmed to cause a request for purchase transaction records to be sent to said payment computer; and

15       said payment computer being programmed to receive said request for purchase transaction records and to cause a document derived from said purchase transaction records to be sent to said buyer computer.

60. A method of operating a payment computer in a  
20 network payment system comprising at least one buyer computer for operation by a user desiring to buy a product, and at least one payment computer for processing payment messages from said buyer computer, said method comprising the steps of:

25       receiving, at said payment computer, a payment message that said buyer computer has caused to be sent to said payment computer, said payment message comprising a product identifier identifying said product that said user desires to buy;

30       causing an access message to be created to enable said user to access said product;

    recording a purchase transaction record in said settlement database;

- 39 -

receiving a request for purchase transaction records that said buyer computer has caused to be sent to said payment computer; and

causing a document derived from said purchase 5 transaction records to be sent to said buyer computer.

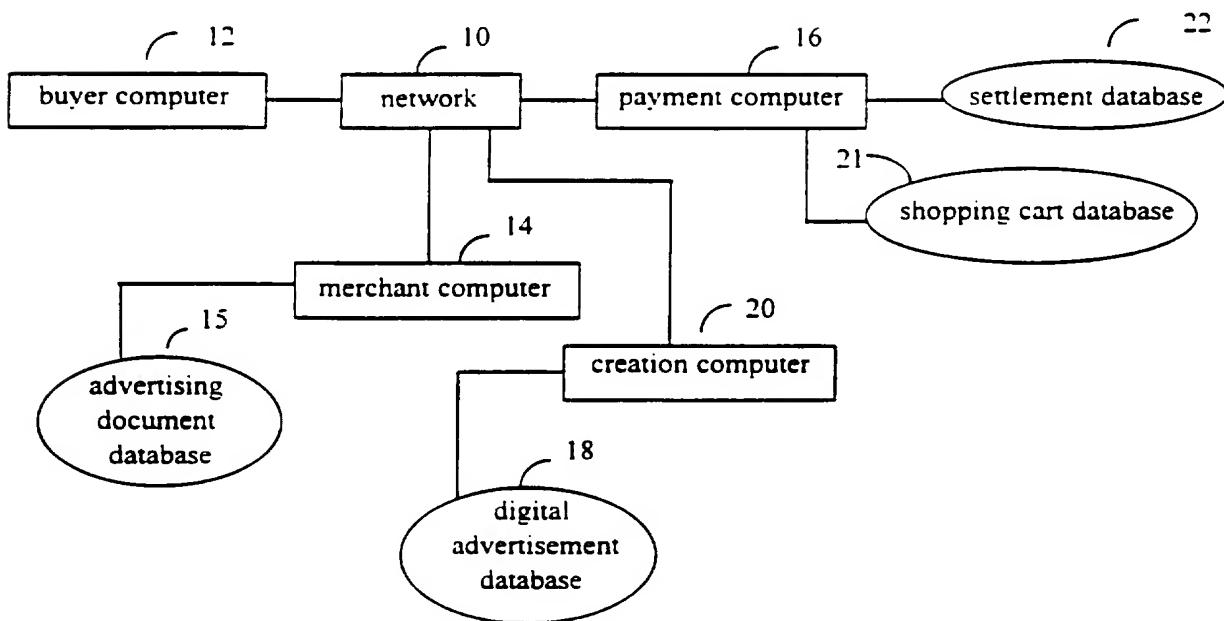
buyer computer 12merchant computer 14payment computer 16

Fig. 1

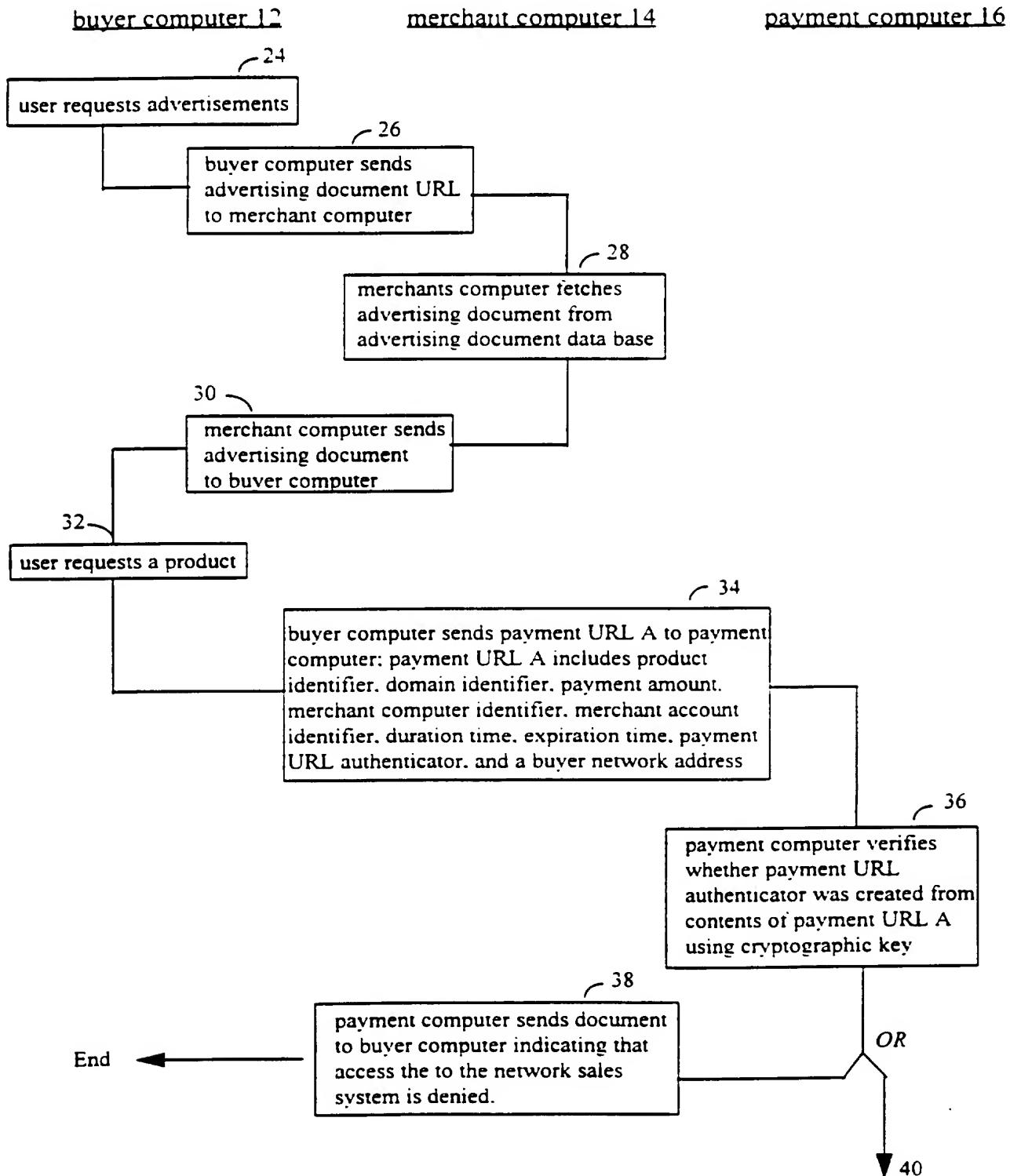


Fig. 2-A

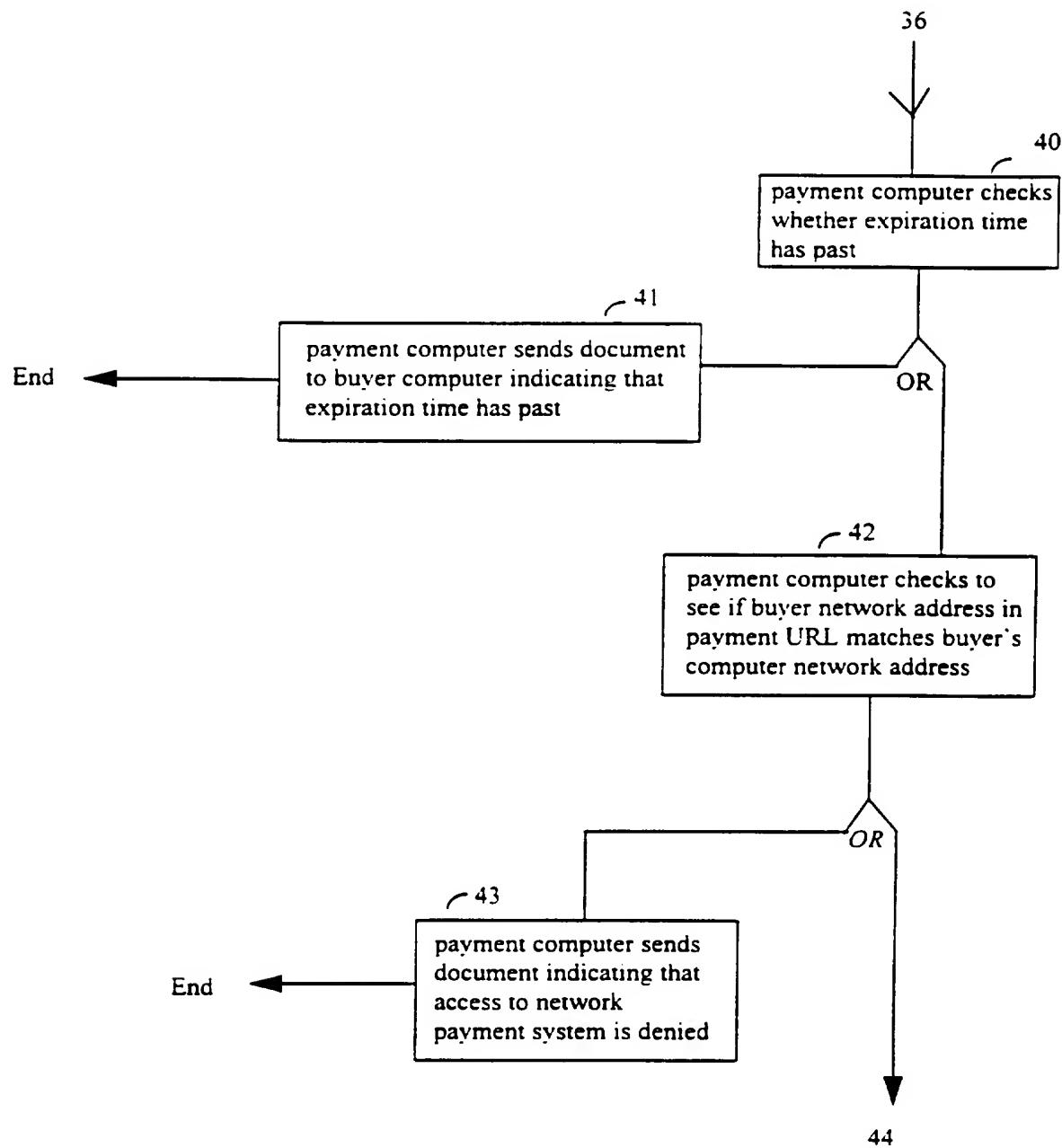
buyer computer 12merchant computer 14payment computer 16

Fig. 2-B

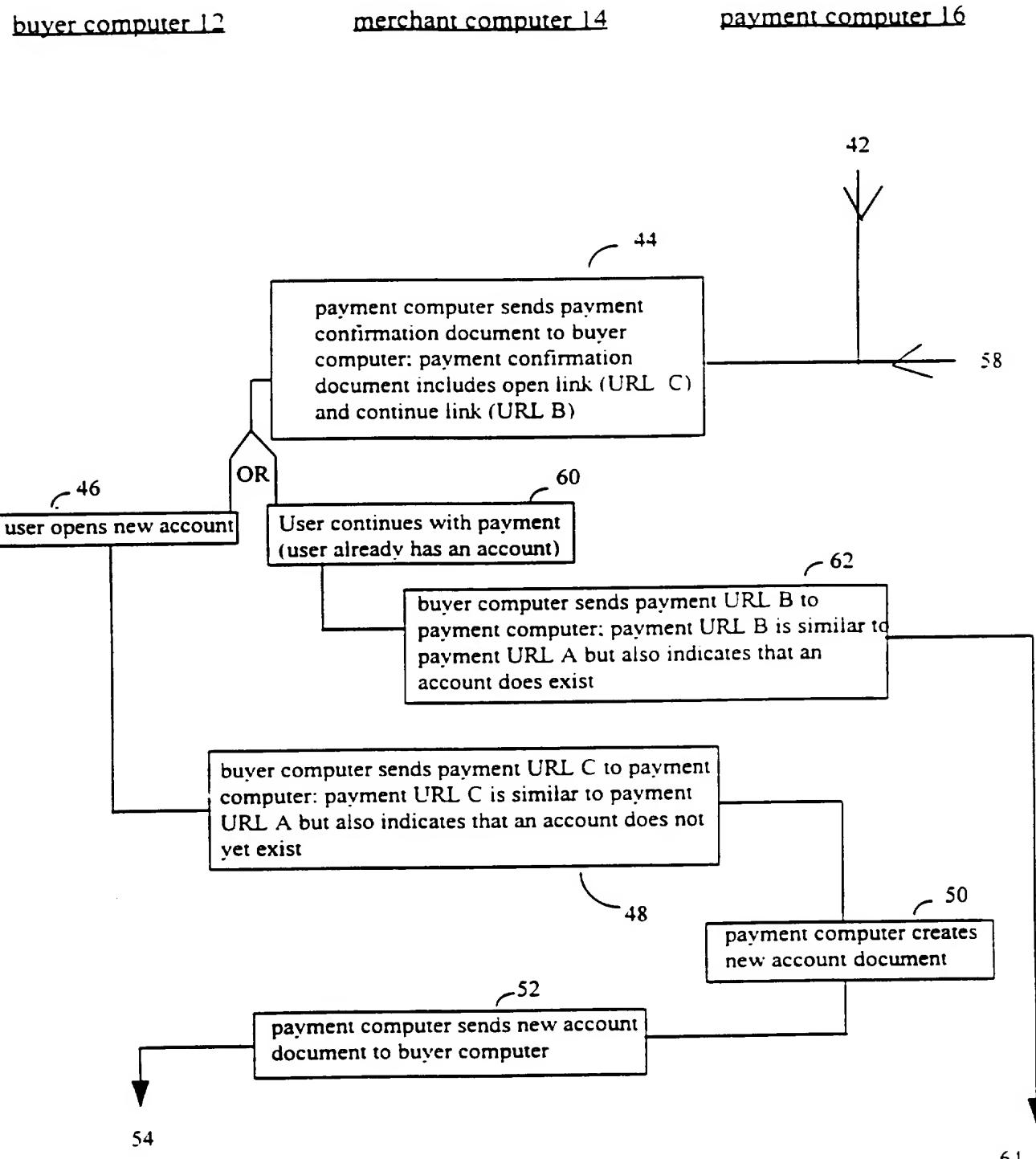


Fig. 2-C

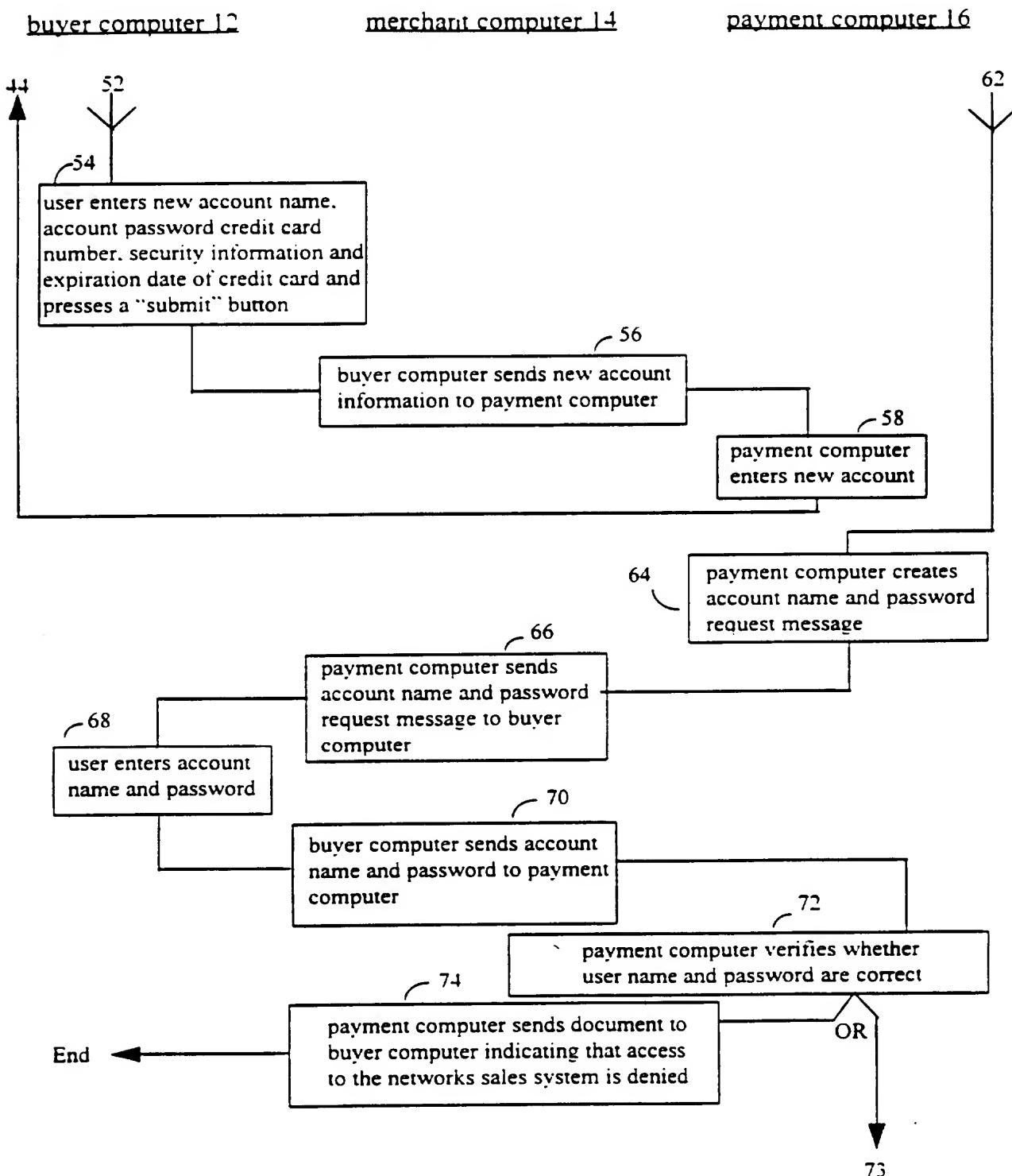


Fig. 2-D

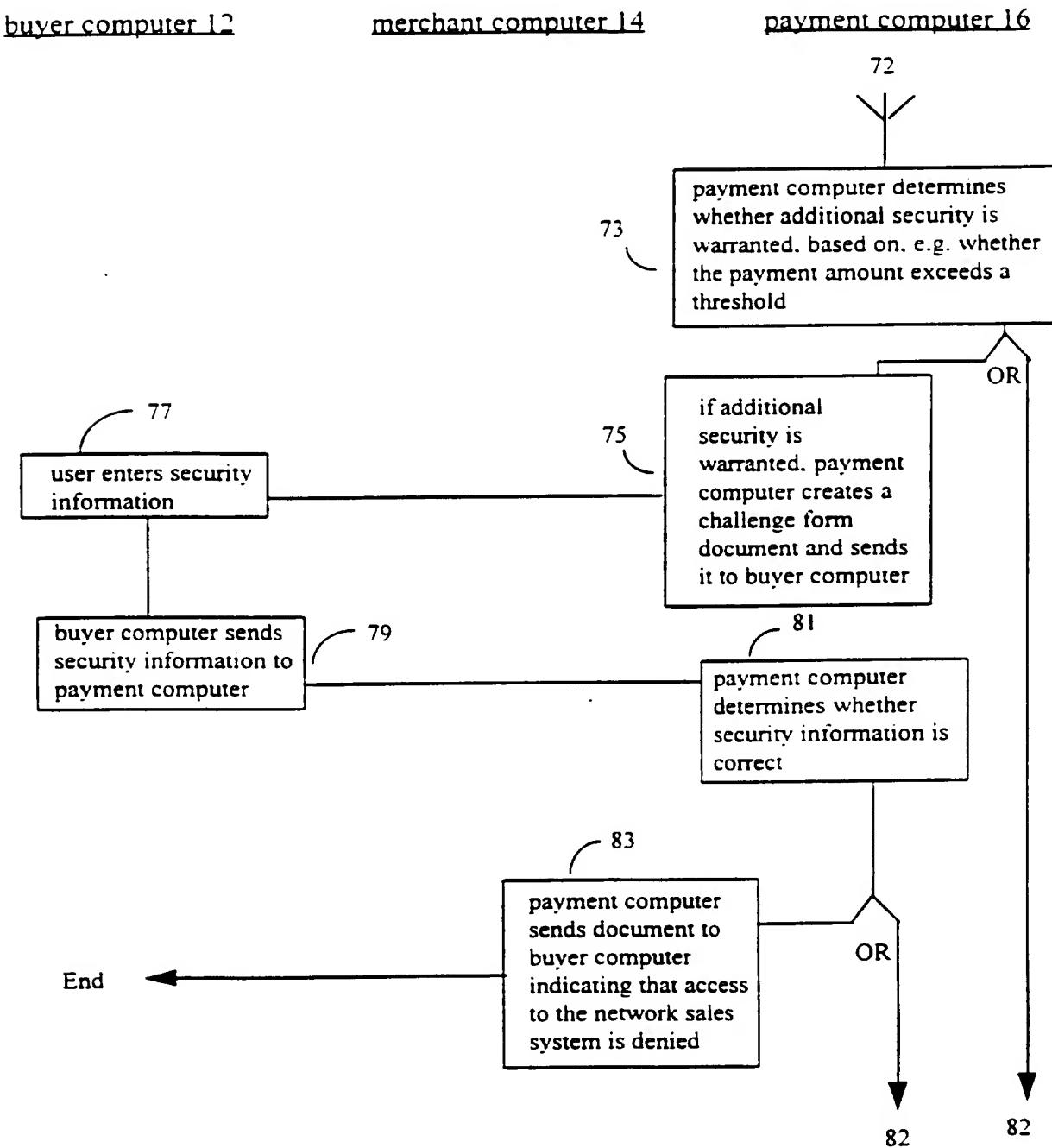


Fig. 2-E

7/25

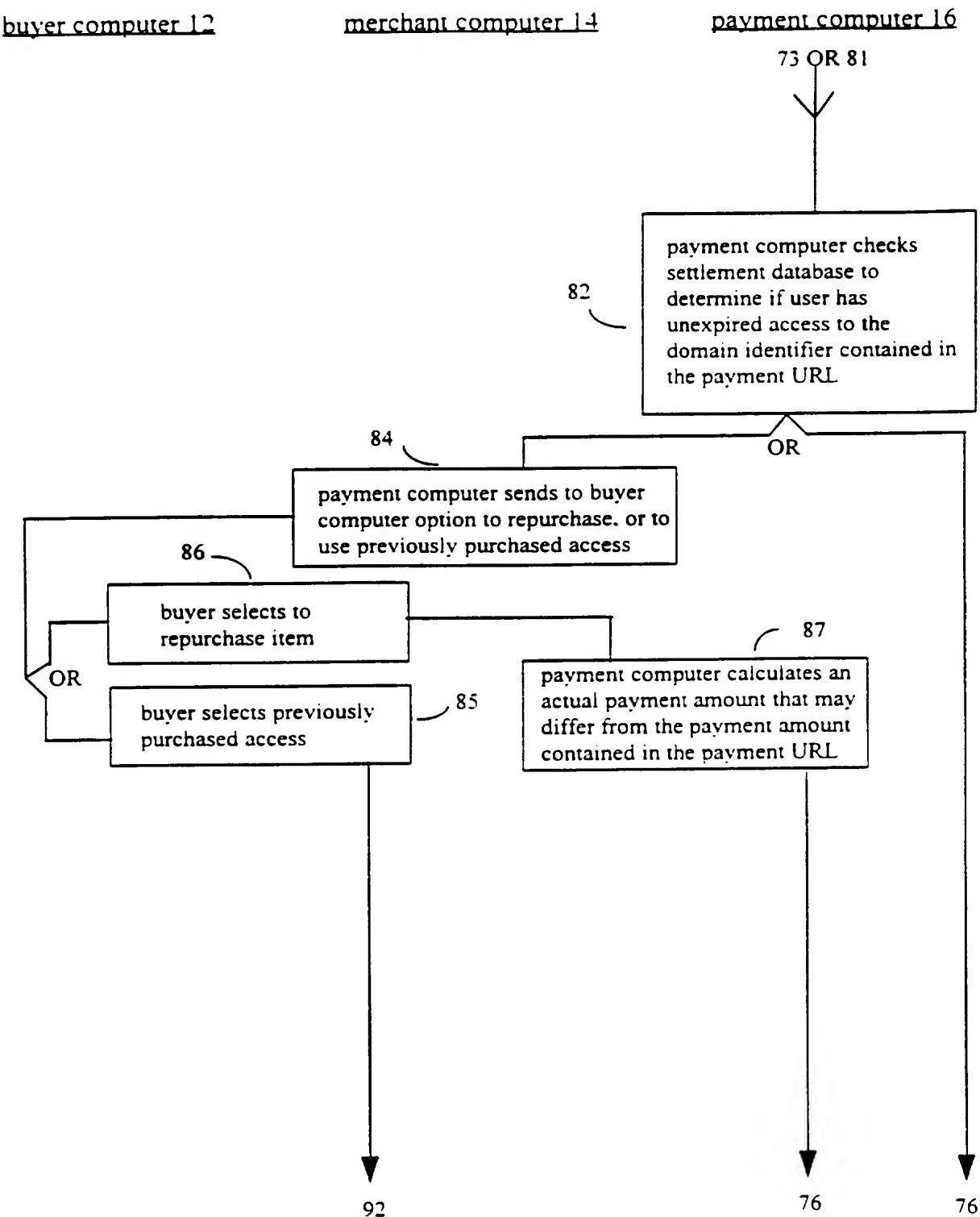


Fig. 2-F

8/25

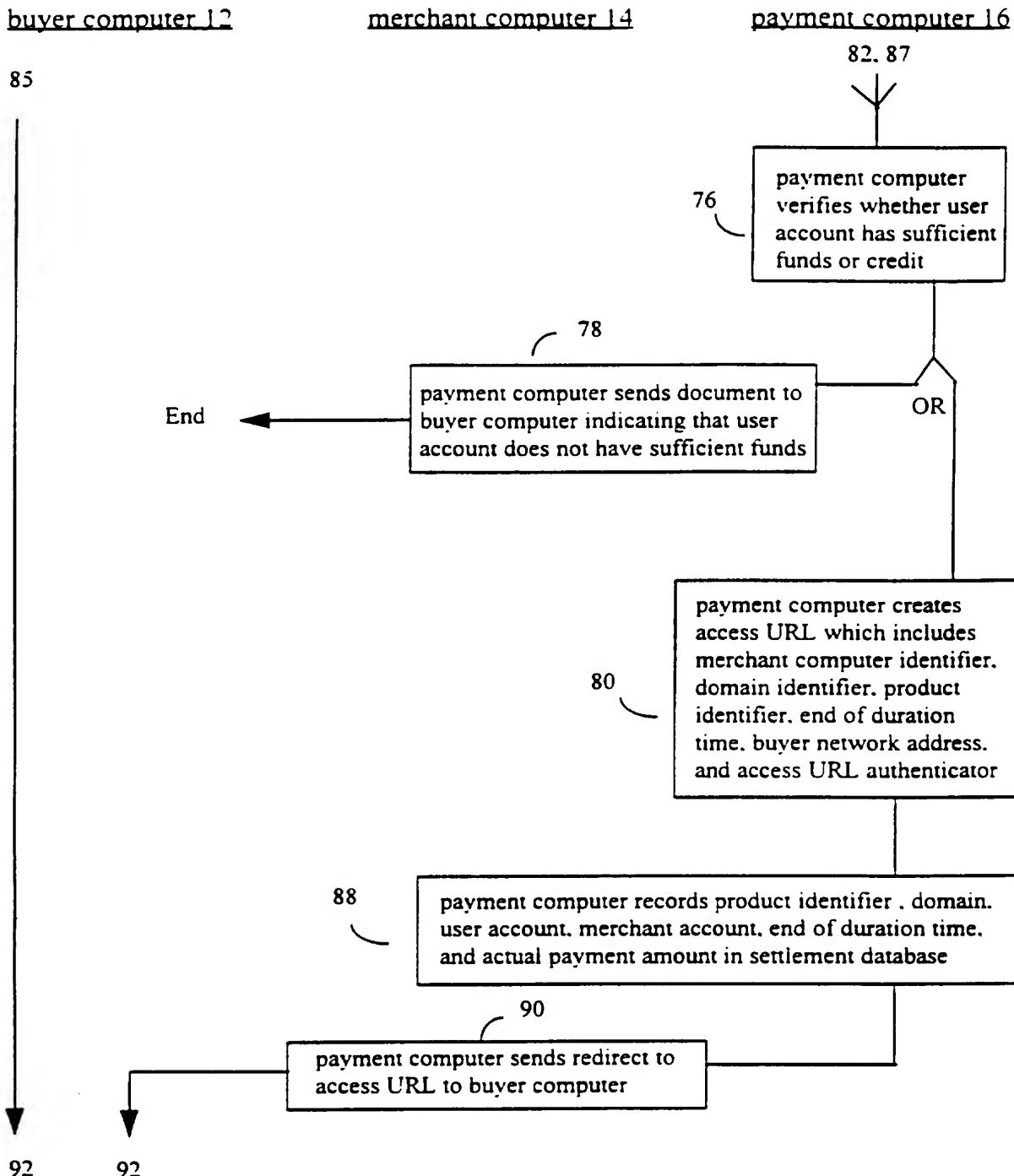


Fig. 2-G

9/25

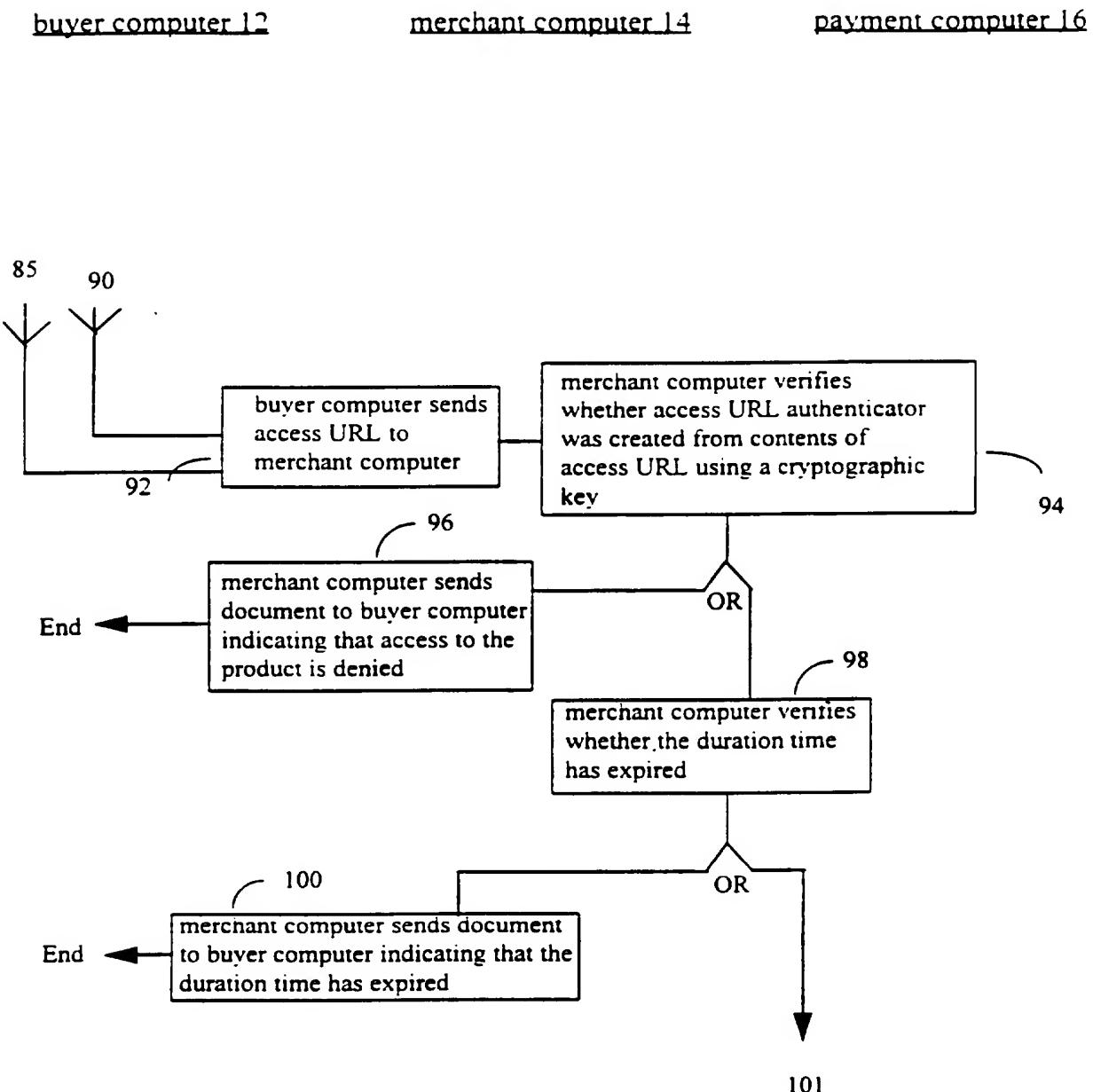


Fig. 2-H

10/25

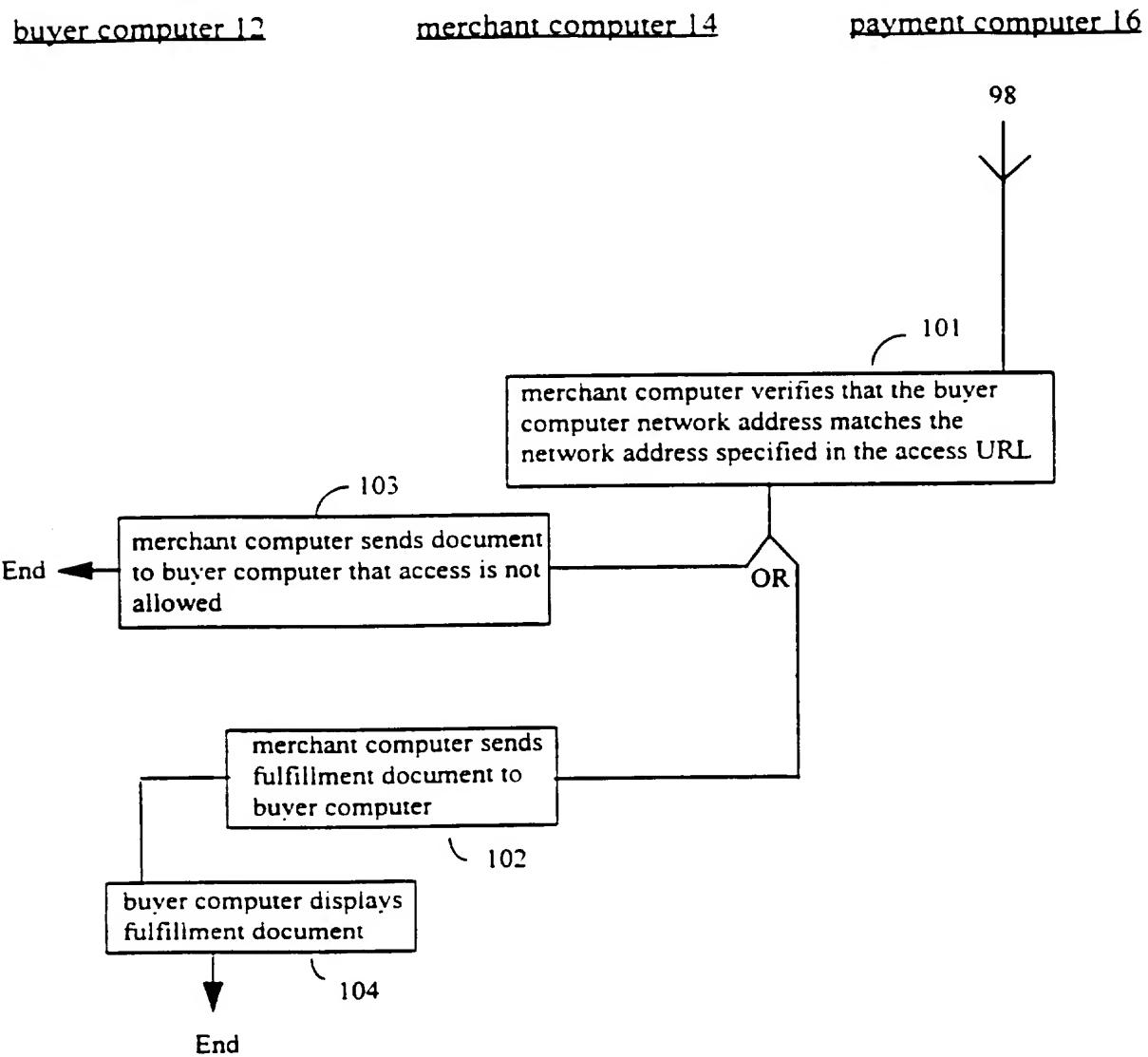


Fig. 2-I

11/25

buyer computer 12merchant computer 14payment computer 16

From 32

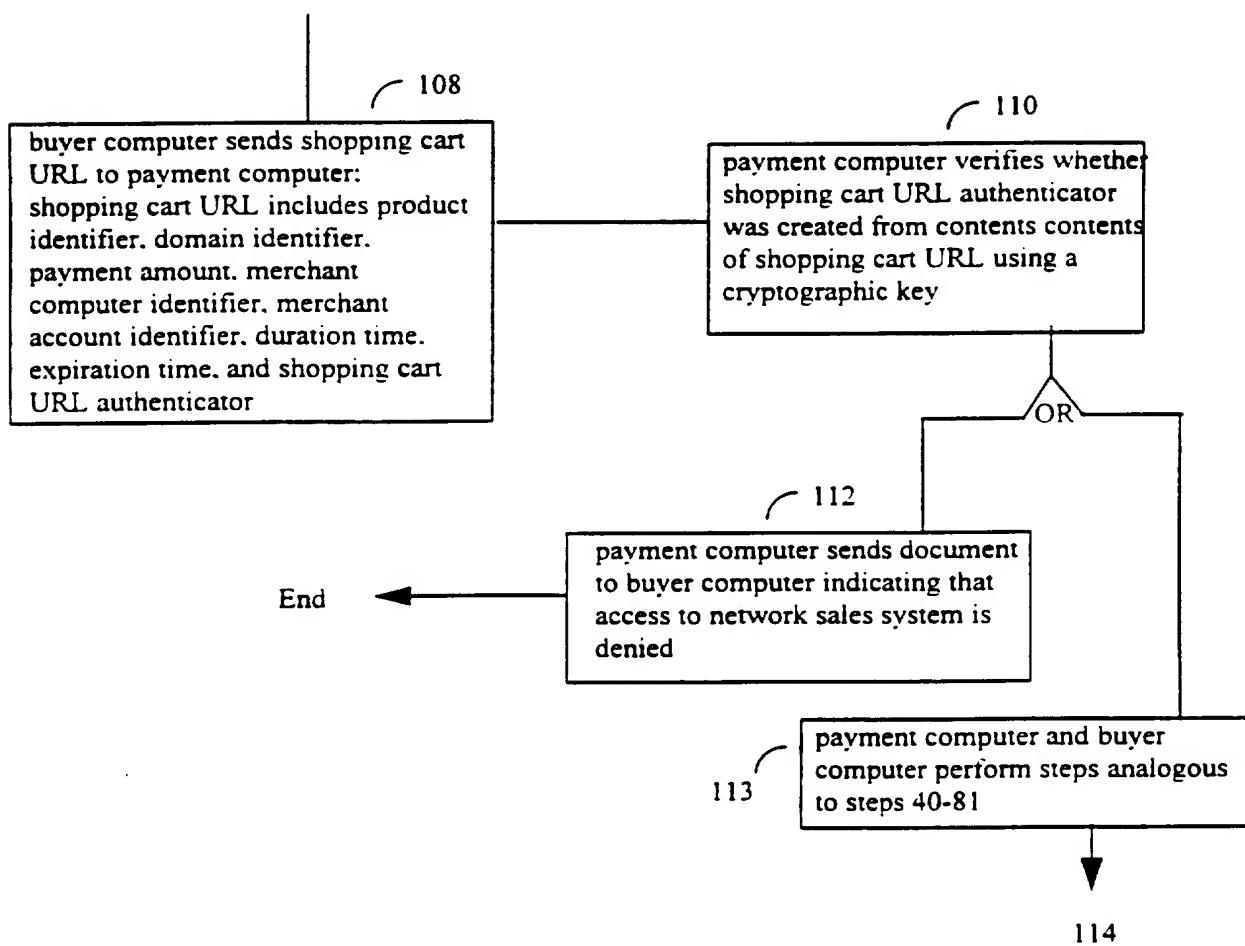


Fig. 3-A

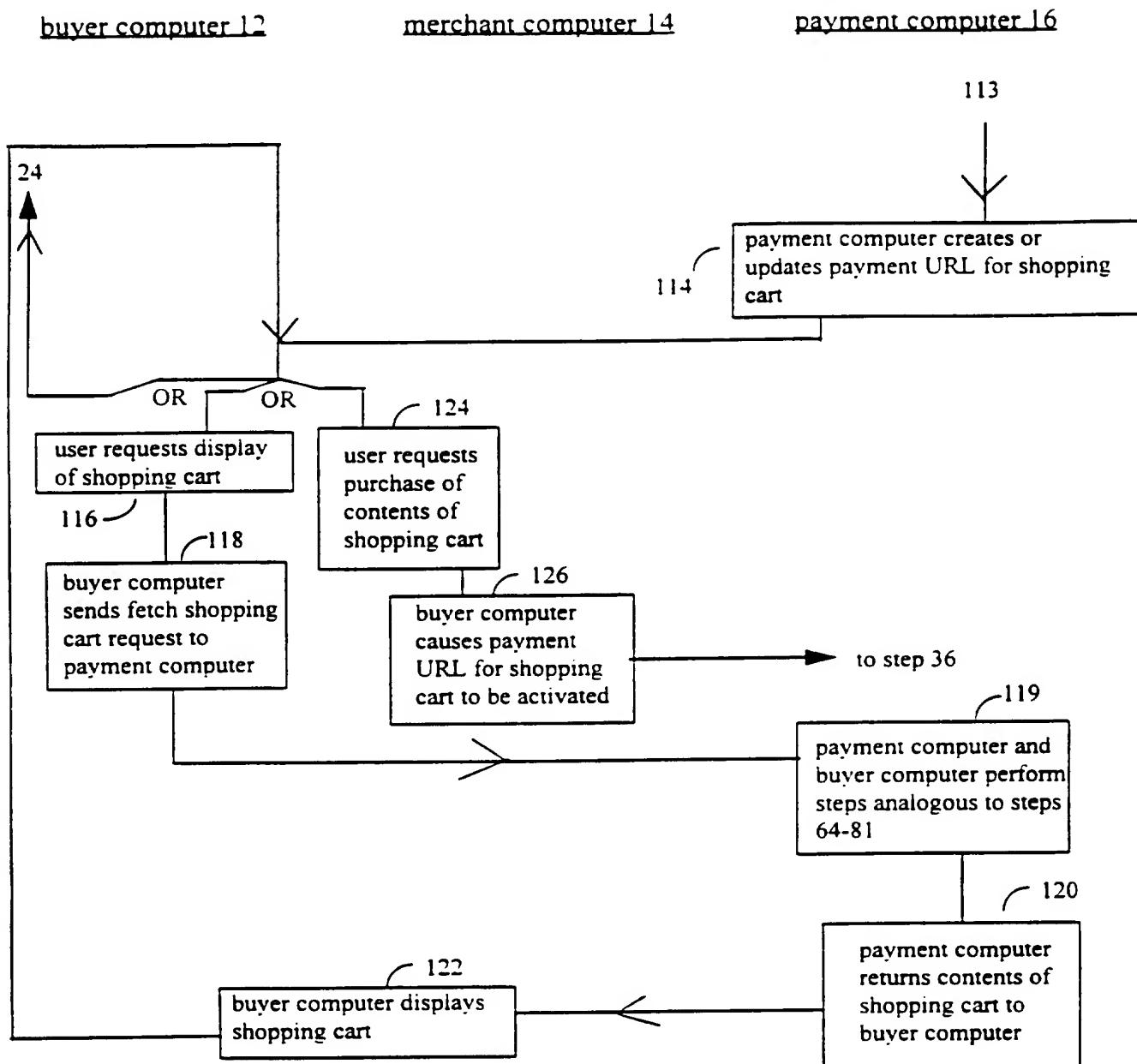


Fig. 3-B

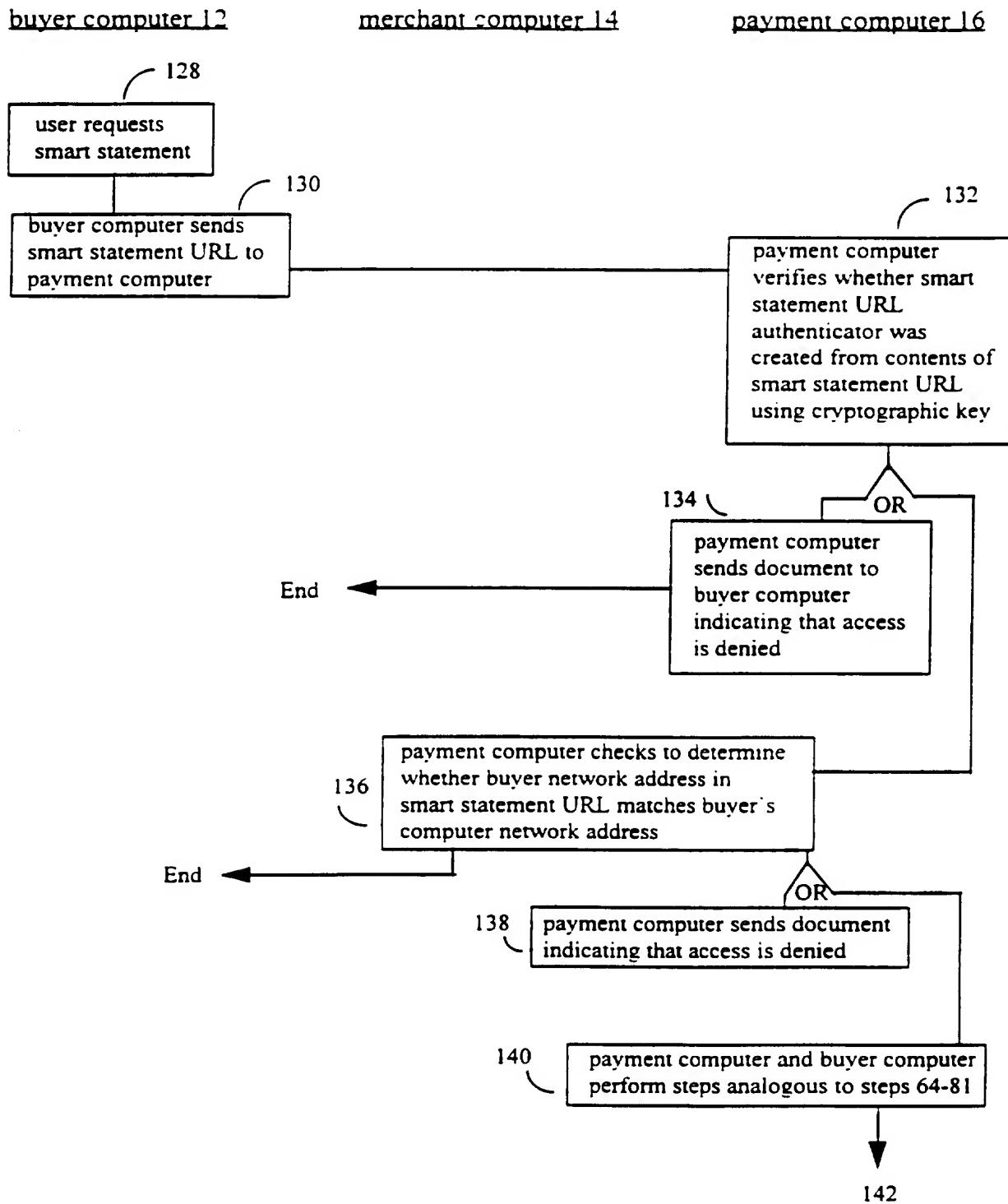


Fig. 4-A

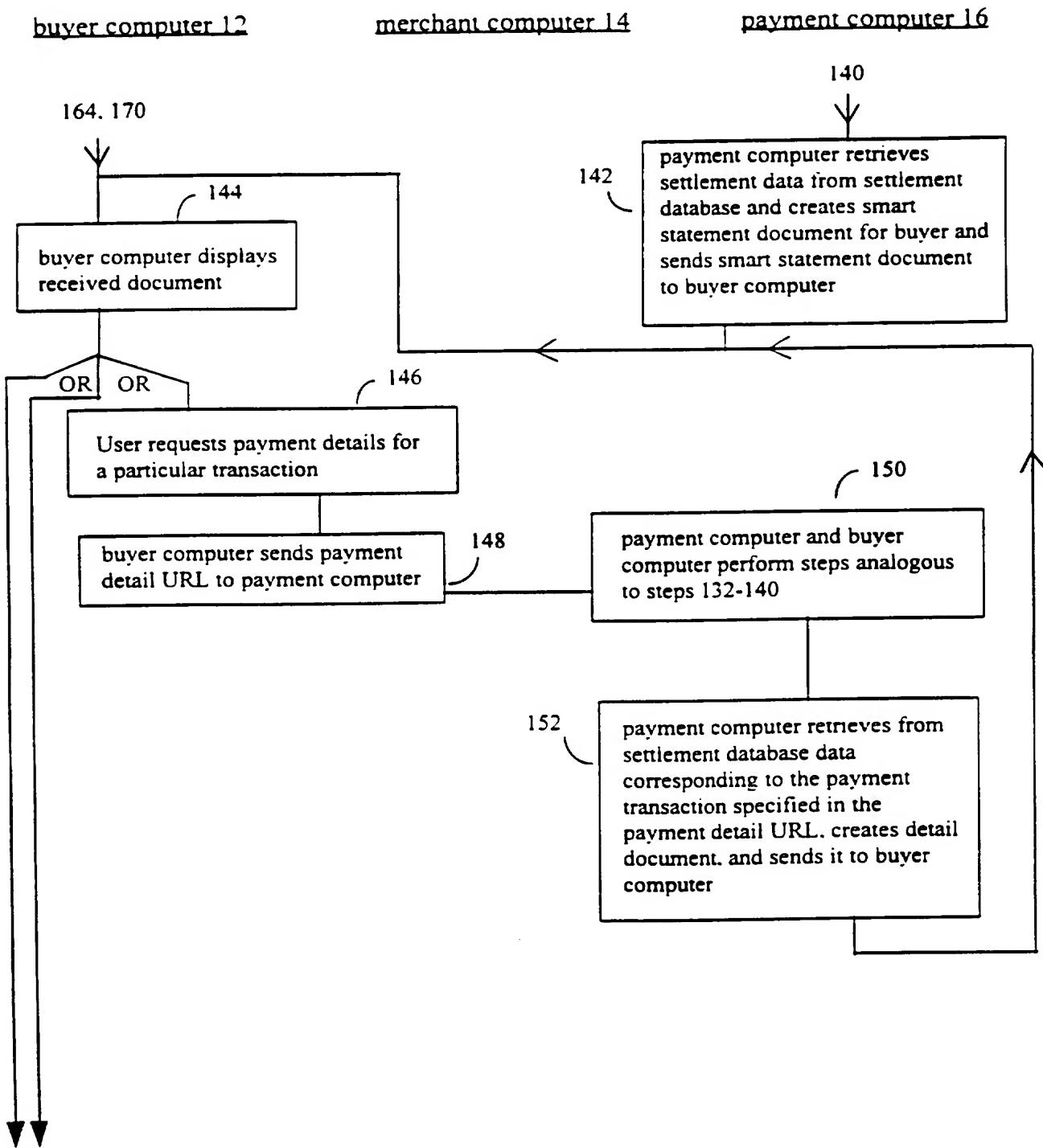


Fig. 4-B

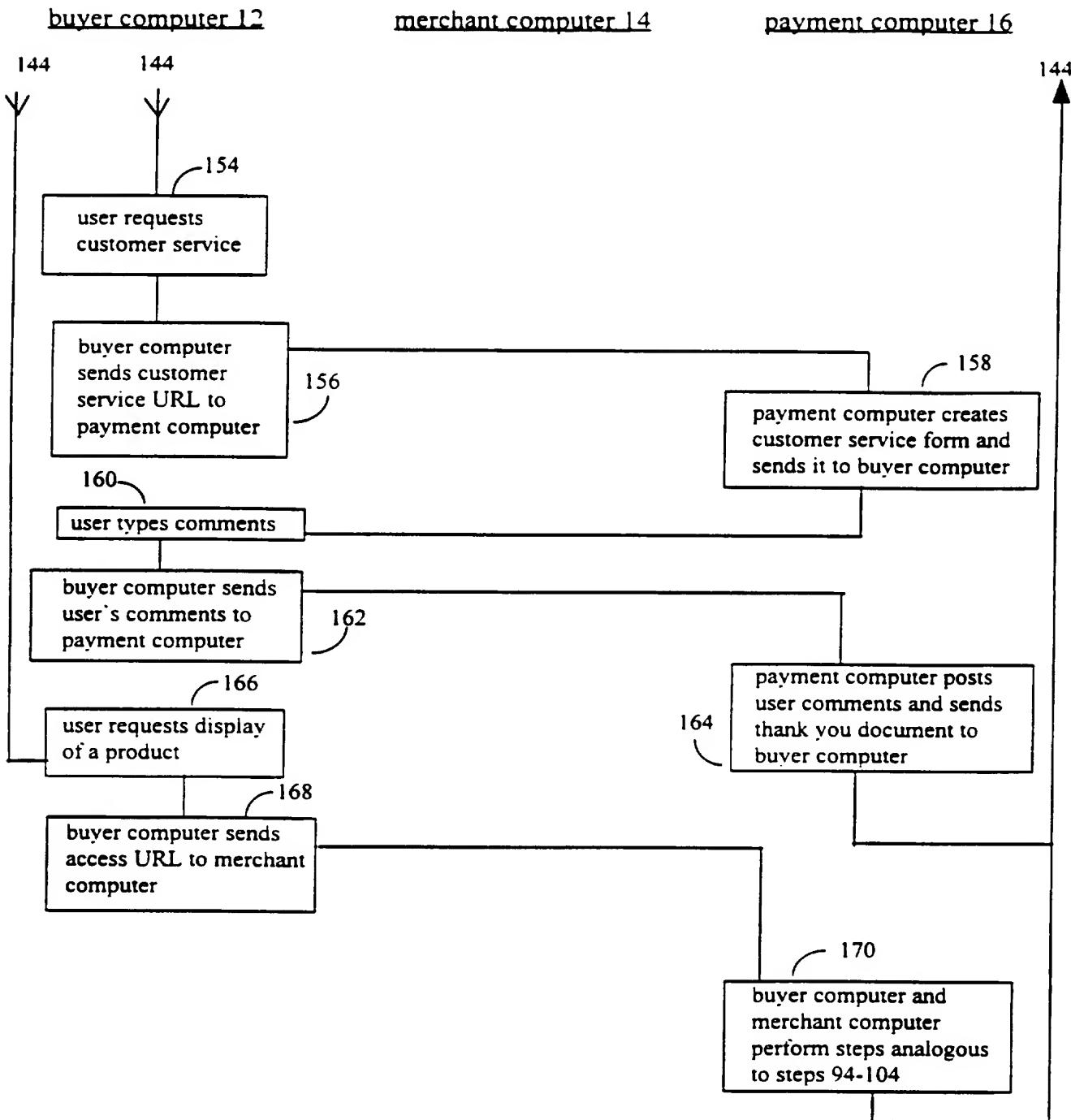


Fig. 4-C

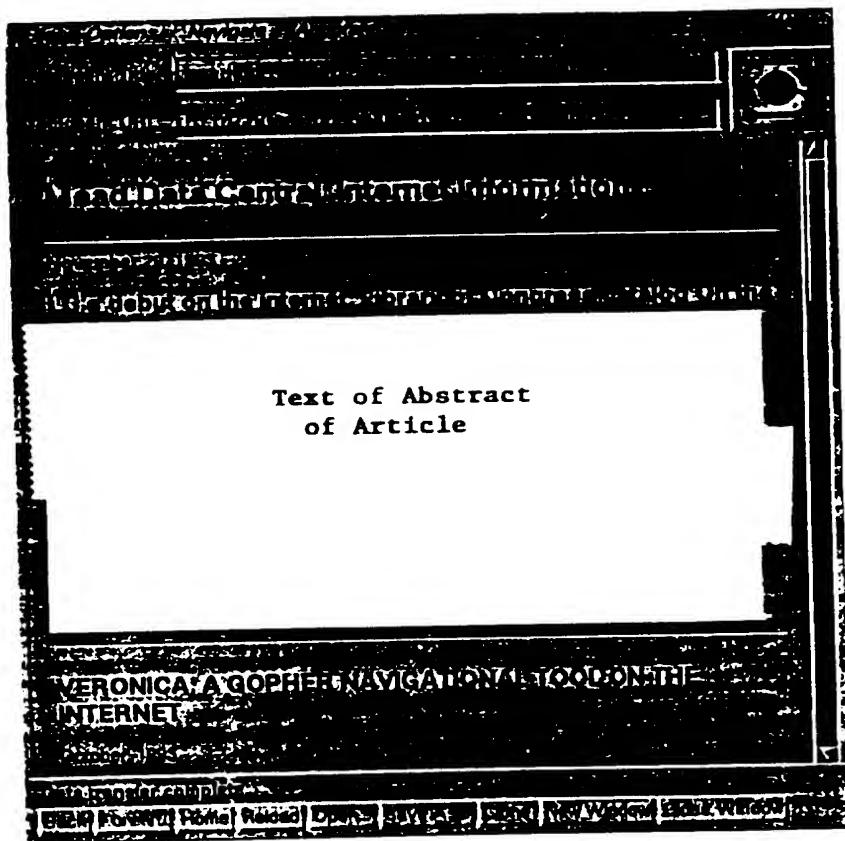


FIG. 5

17/25

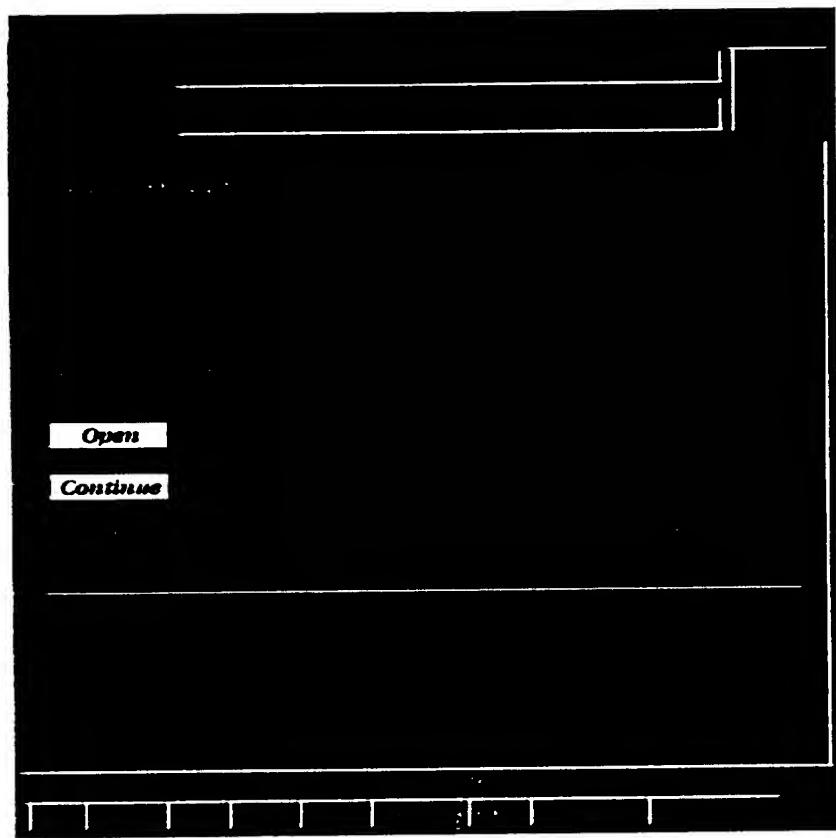
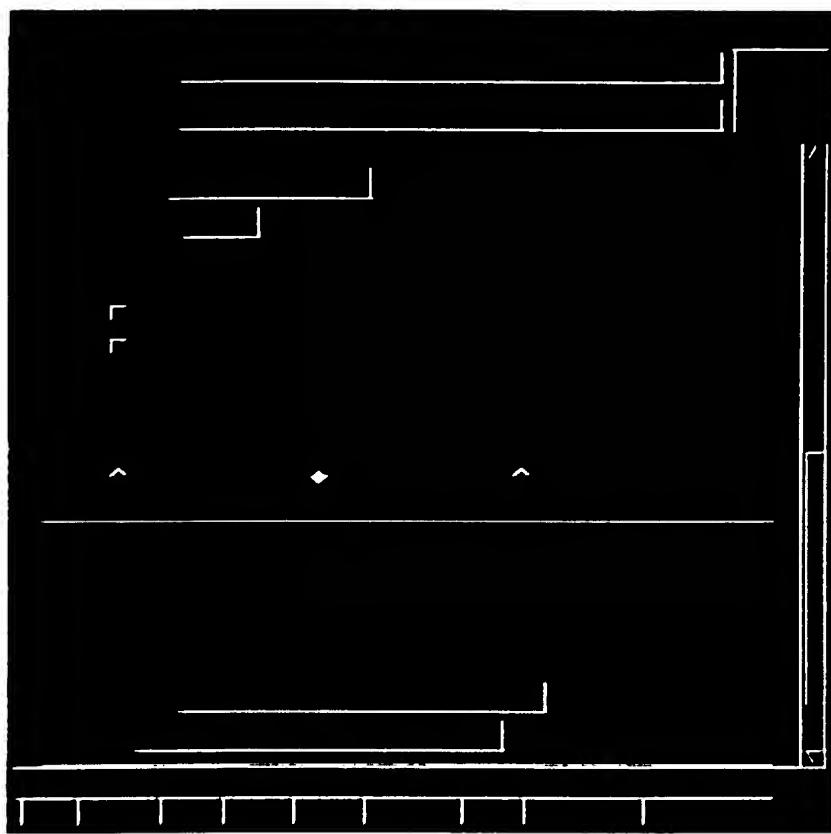


FIG. 6

**18/25**



**FIG. 7**

19/25

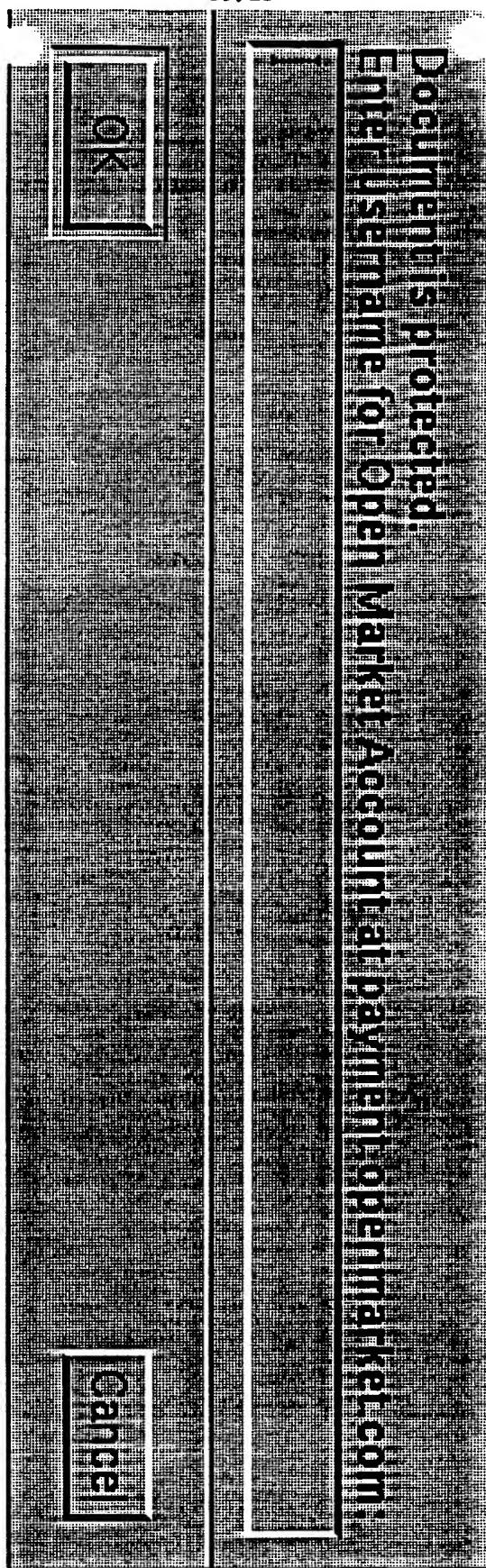
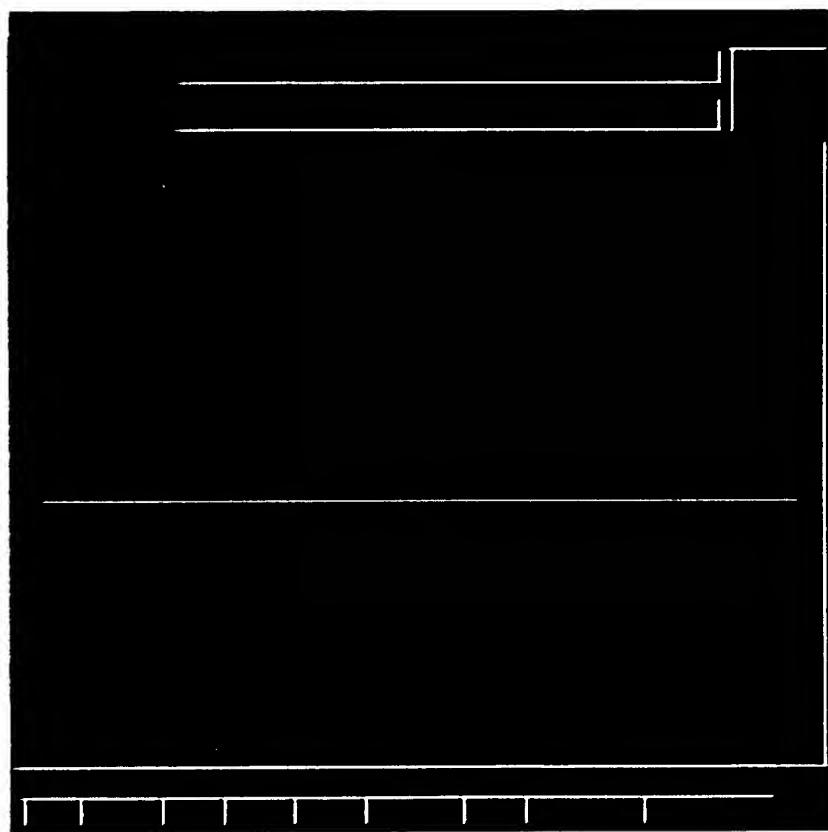


FIG. 8

**20/25**



**FIG. 9**

21/25

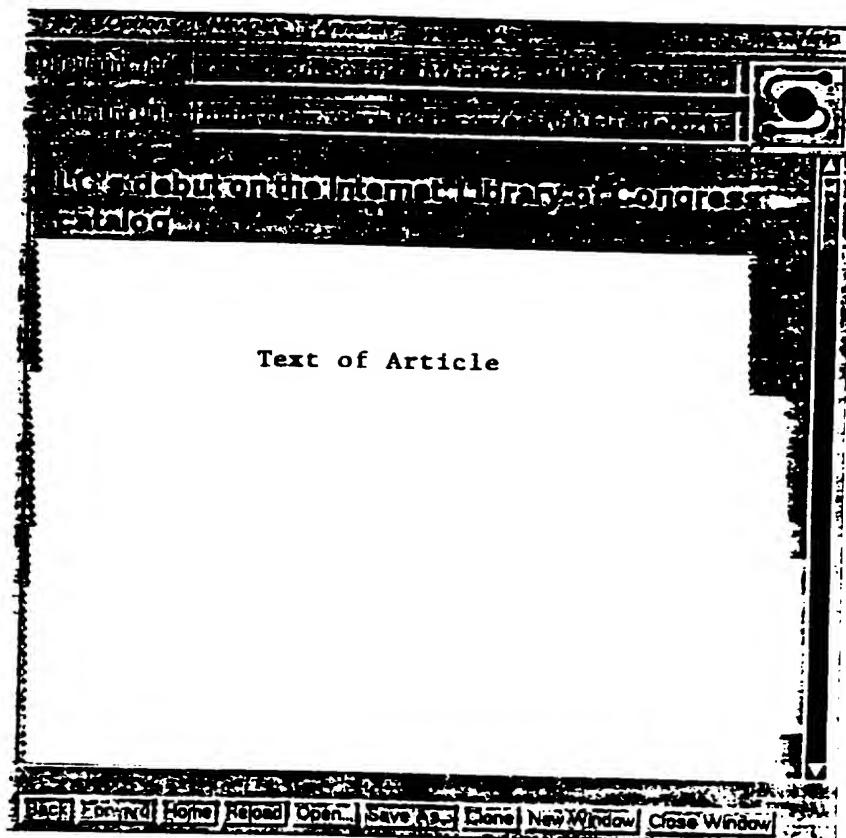


FIG. 10

22/25

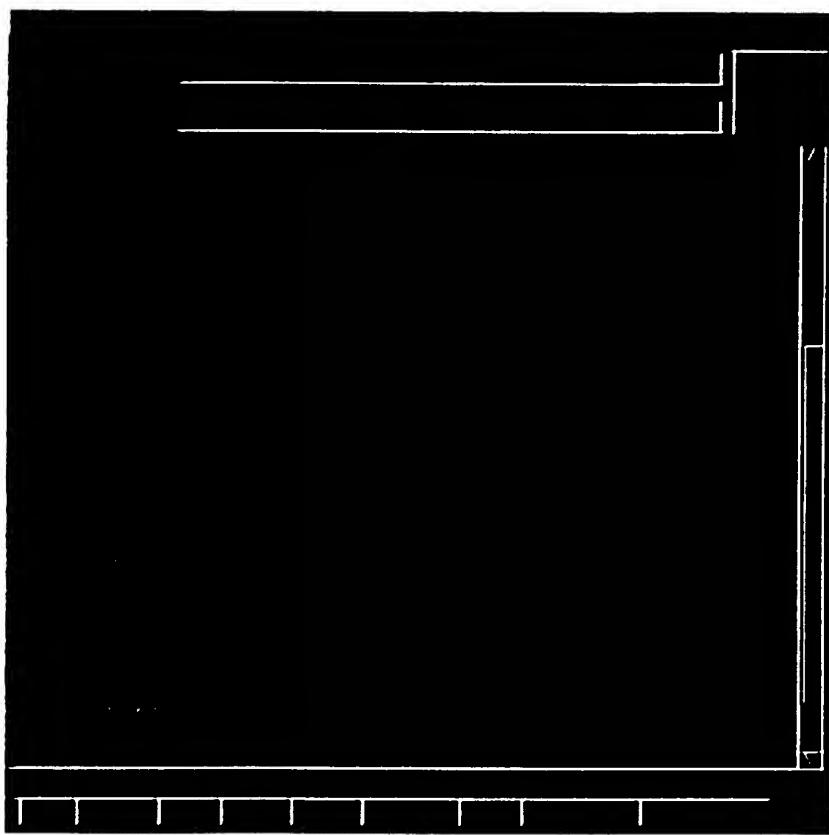
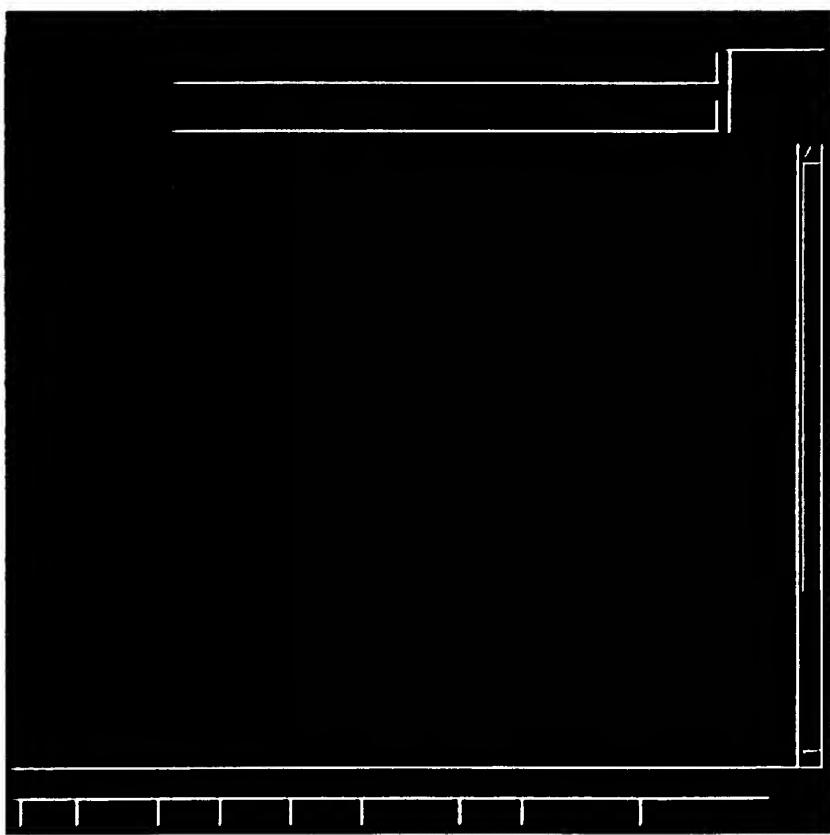


FIG. 11

**23/25**



**FIG. 12**

24/25

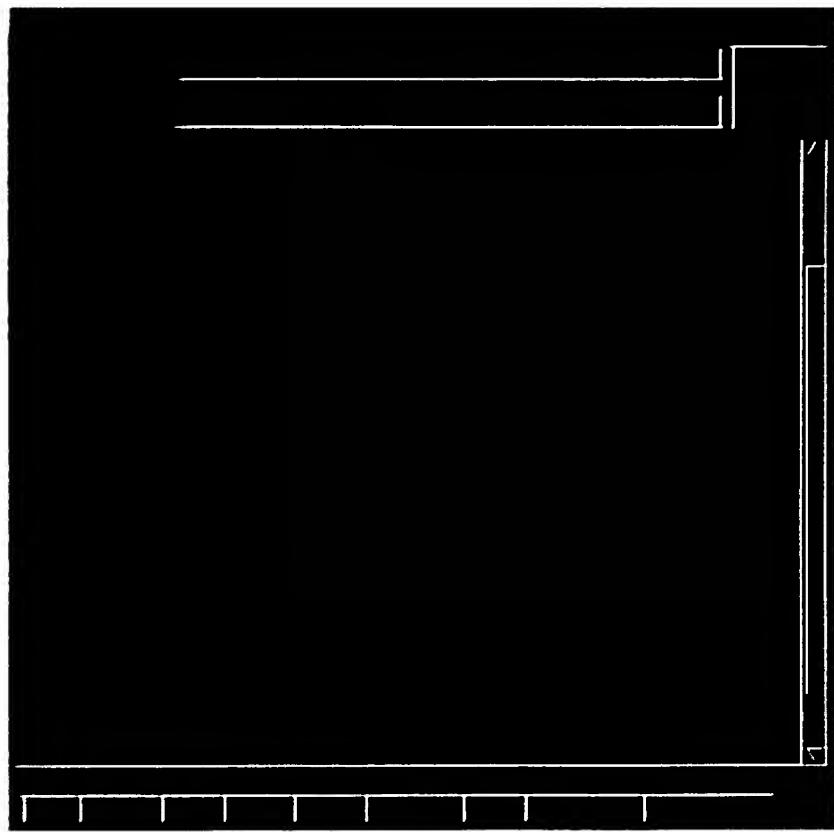
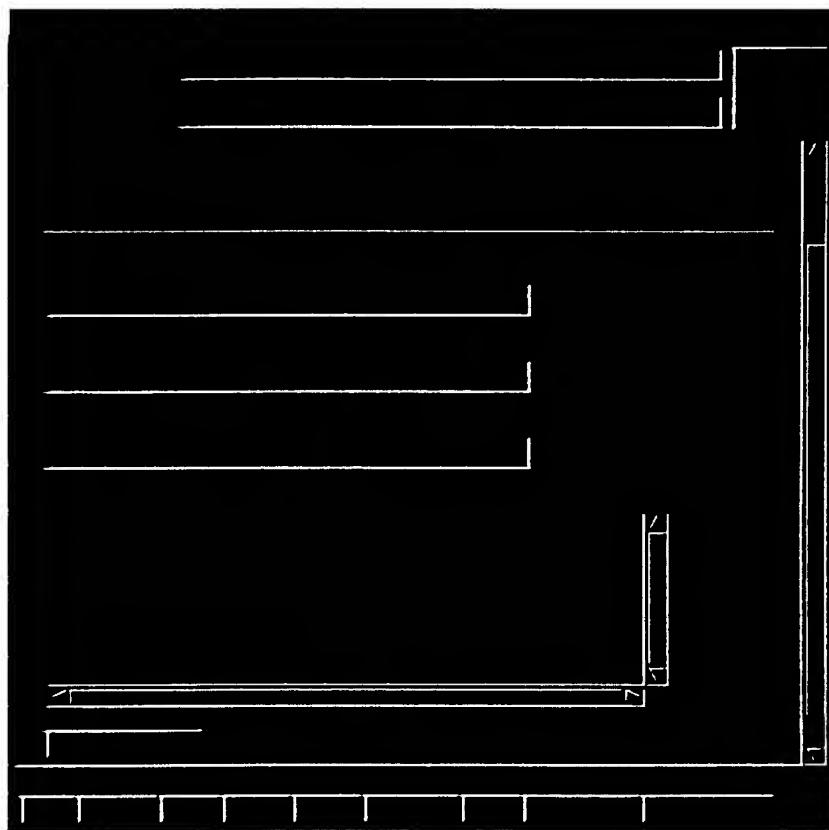


FIG. 13

**25/25**



**FIG. 14**

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US95/13723

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 17/60

US CL :364/401

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 364/401, 406, 408; 340/825.33; 380/23, 24; 902/1, 2, 4

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Dialog database, APS database, Internet particularly <http://www.commerce.net>, Computer Select

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|--|-----------------------|
| Y         | US, A, 4,799,156 (SHAVIT ET AL) 17 January 1989, col. 8-14                         | 1-60                  |
| Y         | US, A, 4,992,940 (DWORKIN) 12 February 1991, col. 1-3                              | 1-60                  |
| Y         | US, A, 4,922,521 (KRIKKE ET AL) 01 May 1990, col. 6, lines 1-52                    | 6, 8                  |
| Y         | US, A, 4,775,935 (YOURICK) 04 October 1988, col. 13-16                             | 34-39, 49-53          |
| A         | US, A, 4,795,890 (GOLDMAN) 03 January 1989, col. 1-2                               | 1-60                  |
| A         | US, A, 4,734,858 (SCHLAFLY) 29 March 1988, entire document                         | 1-60                  |

Further documents are listed in the continuation of Box C.  See patent family annex.

|   |     |  |
|---|-----|--|
| • Special categories of cited documents:  | "T" | later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  |
| "A" document defining the general state of the art which is not considered to be part of particular relevance   | "X" | document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone   |
| "E" earlier document published on or after the international filing date  | "Y" | document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" | document member of the same patent family  |
| "O" document referring to an oral disclosure, use, exhibition or other means  |     |  |
| "P" document published prior to the international filing date but later than the priority date claimed  |     |  |

|   |  |
|---|--|
| Date of the actual completion of the international search | Date of mailing of the international search report |
| 28 DECEMBER 1995  | 15 FEB 1996  |

|   |  |
|---|--|
| Name and mailing address of the ISA/US<br>Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231<br>Facsimile No. (703) 305-3230 | Authorized officer<br><i>GAIL O. HAYES</i><br>Telephone No. (703) 305-9711 |
|---|--|

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US95/13723

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|-----------|--|-----------------------|
| Y         | MIT Laboratory for Computer Science, "SNPP: A Simple Network Payment Protocol", Semyon Dukach, see entire document   | 1-33, 40-47           |
| A,P       | Business Wire, 26 June 1995, "CommerceNet Urges Government to Ease Export Restrictions on Encryption Products; Consortium's New White Paper Articulates Position on the Export of Cryptography-Based Products" | 1-33, 40-47           |
| A,P       | CommerceNet, <a href="http://www.commerce.net">http://www.commerce.net</a> , December 1994, E. Rescorla and A. Schiffman, "The Secure Hypertext Transfer Protocol"   | 1-60                  |
| A         | US, A, 5,220,501 (LAWLOR ET AL) 15 June 1993, entire document  | 1-60                  |